MORLEY ELECTRONICS LIMITED

VISIKEY User manual & Installation Guide

© Morley Electronics Ltd.
Unit 34, Moorland Way, Nelson Park, Cramlington,
Northumberland, NE23 1WE
Tel: +44 (0) 1670 732444
Fax: +44 (0) 1670 707333
Email: accesssales@morleyuk.co.uk
Web: www.morleyuk.co.uk

Table of Contents

Chapter One 1
Overview of the VISIKEY ... 1

Chapter Two 3
Features and Specifications .. 3

Chapter Three 7
Operating Methods 7
Use of a Keycard 7
Use of an Infra-red Tag 7
Review 8

Chapter Four 9
Computing Requirements 9
Computer specification 9

Chapter Five 11
Software Installation 11

Express Install 11

Chapter Six 13
Changing Passwords 13

Chapter Seven 15
The System Menu 15
Who is Logged On? 15
Enabling Other Operators 15
Quit 16
Restart 16
Shut Down 16
Environment 16
Force Backup 18

Chapter Eight 19
The CONFIG Menu 19
Day Types 19
Week Types 19
Year Types 19
Holidays 19
Departments 19
User Fields (see fig. 9.2) 21
Titles 21
PIN Algorithm 21
Fig. 9.3 Title, PIN Algorithm, Monitor Control and Capacities Windows. 22
Time & Attendance Reason Codes 23
Time & Attendance Output 23
Area Names, APB and Capacity 23
Capacity List 23
Loops and Readers 23
Reader Logic 24
Reader Resources 24
Reader Keypad Layouts .. 24
Reader Technologies 24
Interconnectivity 25
Codes for Global Scripts. 25
Floor Plans 25
Alarm Messages 26
Alarm Windows 27
Alarm Sounds 28
Monitors and Outputs 29
COMMs Port I/O 29
Sub-area configuration ... 30

Chapter Nine 33
USERS Menu 33
Create User(s) 33
Find User 33
Pack User Base 33
Group user changes 34

Chapter Ten 37
MONITOR Option 37

Chapter Eleven 39
LOGIN Menu 39
Change Password 39

Re-login.....39
Logout.....39

Chapter Twelve.....41
CONTROL Menu.....41
Plans and Maps 41
Zoom Control.....41
MROC all loops 41
MROC a loop.....41
MROC an Area 41
MROC a reader.....41
Area Info 41
Reader Info.....42
Reset MUXs.....43

Chapter Thirteen.....45
History Recall.....45
History File to Search 45
Start and Stop times 46
Search on Particular Group 46
Search on Textual Content (Wild card).....46
Alarm Occurrences and Acknowledgements.....46
Departmental Search.....46
Search When a Certain Operation is Present.....46
Reader 46
Area.....46
Keynumber.....46
Technology 46
Transaction.....47

Chapter Fourteen.....51
System Configuration in Detail 51
Defining Day Types.....51
Defining Week Types 53
Defining Year Types.....54
Defining Areas.....54
Defining Departments and Their Access Rights.....55
Defining User Fields.....57
Entering a New Card Holder 59
Textual Information 59
Yes/No Information 60
Drop Menu' Information.60
Button Click Information 63
Use of the Holiday Information Windows..... 64
Use of the Monitor Window 67

Chapter Fifteen.....69
Planning Your System 69

Chapter Sixteen.....69
Programming a Reader..... 69
Entering a Program..... 69
Writing a Program 72
Operators..... 74

Appendix 1.....77
Boolean Algebra (RPN)..... 77
Reverse Polish Notation (RPN)..... 79
Example script program.. 80

Appendix 2.....83
Plan and Map Script Language 83

Appendix 3.....84
Glossary of terms 84

Chapter One

Overview of the VISIKEY

The VISIKEY from Morley Electronics is an efficient and highly effective system designed for building access control and management. By controlling the system using an IBM or compatible personal computer, maximum flexibility has been achieved whilst retaining ease of operation. The VISIKEY can be custom configured to suit your needs and as these needs change, so can the VISIKEY.

A simple pointing device such as a mouse or a trackerball is all that is needed to control all of the VISIKEY functions through its sophisticated windows driven software. Once installed this software allows you to configure the system to your own needs. The VISIKEY software can be used to control access to selected areas of buildings using both physical and temporal constraints. It can also control and be controlled by other building systems such as fire alarm/control systems or burglar alarm systems through its versatile, digital interfacing system. Both fail-safe and/or fail-secure environments can be implemented.

The VISIKEY software allows multi-tasking. With multiple control windows on display, all updated in real-time, the VISIKEY user can ensure safe, efficient and secure access control management at all times.

Chapter Two

Features and Specifications

Using sophisticated software VISIKEY gives you the precision control you need for effective access control management. The window-driven programming allows you to accomplish every task with a few simple 'point and click' operations. The entire system can be easily configured to suit your own needs. Readers may be addressed globally, in pre-selected groups, or individually. These operations can be carried out via menu selection, through pre-programmed event control (e.g. security alarm), or by control through the site plan windows.

Areas within a site may have an Anti-Passback (APB) level associated with them, giving added security by preventing the use of the same Key twice in any one Area. Using APB the building plan can be viewed as a series of nested boxes. Access is only allowed to the next level if all previous levels have been passed. Also, a person may not re-enter an APB Area unless they have already left it, i.e. cards cannot be passed back through windows etc. for re-use by another colleague.

Areas can have configurable capacity limits. When reached, these stop all further attempts at entry. Such a system is very useful with regard to compliance with fire and structural regulations.

The site plan allows real-time monitoring of the status of door-readers, with more detailed information available with a single pointer operation. Any reader within the plan window may be overridden remotely through the software. Readers, or groups of readers, can also be subject to remotely controlled manual override via simple mouse clicks if this should prove to be necessary.

Key-holders can be tracked through the building in real-time. Their access rights to building areas can be altered immediately or when appropriate, giving immediate results. Each key-holder is assigned to a Department, which in turn has certain specified access rights to different Areas at different times of day, week and year. These may be overridden by Holiday Information, which allows each department to be assigned different access rights on particular days of the year.

Key-holders can be set to 'time-out' at a particular time and date, rendering their key inoperative after a specified time, but retaining their details within the system.

Along with essential key-holder information, the System User may configure the key-holder database to have fields which are unique to the users application. Each key-holder may be assigned to be a visitor, or a first-aider, or any other class of person the application requires. Each key-holder may have eight yes/no pieces of this type of information held about him/her. Search criteria can also be any other piece of key-holder information e.g. search by surname.

Door Processing Unit (DPU - e.g. card- or tag-reader/controller) operation is configurable by the use of reader scripts. These allow the system operator to control reader outputs and system alarms which may also depend on other inputs and timers. Reader integration into the system is through defining relationships between reader events and system functions.

Any alarm condition, key transaction or console activity may be sent to a real-time window, remote display terminals, printers, files and/or other computers through a RS232 port. Each output device can be configured to display only information in a particular group e.g. only alarm conditions.

The VISIKEY specification is as follows:

• Number of doors	512
• Number of readers	512
• Number of key-holders	65,000
• Number of day types	32
• Number of week types	32
• Number of year types	32
• Number of physical mapped areas	128
• Number of digital inputs	1024
• Number of digital outputs	3072
• Number of DPUs	128
• Number of slave terminals (Multi-User)	7 + Host
• Holiday schedule	Yes
• Password control	Yes
• Anti-Passback	Yes
• Program supervision	Yes
• History recall	Yes
• Colour graphics	Yes
• Programmable alarms	Yes
• Area accounting	Yes
• Plans and maps	Yes
• Multiple reporting/monitor output	Yes
• Full override on individual readers	Yes
• Full override on individual areas	Yes
• Full override on individual loops	Yes
• Full override on whole system	Yes
• DPUs have Time Dependencies	Yes
• Keyboard-less operation	Yes
• Programmable DPU script language	Yes
• DPU interaction with other systems	Yes
• Localised process control	Yes
• Real-time reader information	Yes
• Real-time Area information	Yes
• Real-time key-holder tracking	Yes
• Configurable key-holder information	Yes
• Time and Attendance collection	Yes
• Prioritised alarm windows	Yes
• Muster dumps	Yes
• Configurable alarm sounds	Yes

Supported technologies (supported concurrently) on new Morley NEXUS DPUs:

- Thorn EMI Watermark
- ABA track 2
- Wiegand
- PAC

All technologies which use either a Watermark, Wiegand or SoftMagnetic hardware interface. All bit formats within a Keycard may be specified using the VISIKEY's powerful *Soft Format Configuration* system

Chapter Three

Operating Methods

Keycards, infra-red (IR) tags and Wiegand, amongst other technologies (contact Morley Electronics for further details) can be used with the VISIKEY. Users may also be assigned Personal Identification Numbers (PINs) to be entered into door processing units (DPUs) fitted with keypads. It is not necessary to fit all DPUs with keypads. Users with PINs will still be able to use those DPUs without keypads. The PIN is an added security feature and may only be required for access to certain areas, preventing the use of card stealing.

Pressing 'E' while a card is present in a reader signifies that the user is acting under duress (the Duress button). Use of this by ANY user can be programmed to activate a pre-configured alarm which alerts the system operator, allowing him/her to ensure that the correct action is taken.

Use of a Keycard

WARNING: Users should not insert any cards other than their Key cards into the card-reader mechanism. Other cards e.g. credit cards, may be wiped of information by the system rendering them useless. This is a security feature which prevents the use of programmable cards by persons seeking to gain fraudulent access to a site.

A user wishing to gain access to a certain Area first inserts their Key card into the slot in the card-reader. The user will now, if applicable, type in a PIN, and if this is also valid the card is then removed.

Alternatively, the card may be removed from the reader before PIN entry, but the PIN must be entered within 10 seconds before the card read times out.

The LED fitted to the reader will then display either red or green. If the LED shows green, the card has been recognised as valid and the door will be released. If the card-reader LED shows red then the card is invalid and the user cannot pass. The use of an invalid card is notified to the operator who may then take action as necessary.

Use of an Infra-red Tag

Users with infra-red tags use them by simply pointing them at the relevant point on the tag-reader (signified by a flashing LED) at a distance of approximately 6 inches or less. It is not necessary to specifically operate the tag in any way e.g. to press a button or such like, as the tag is automatically interrogated by the reader.

A steady green light indicates correct operation, while a flashing green light indicates either a misread or a illegal attempt to gain entry.

Review

Both the Keycard and the IR-tag use the same system to identify users. This consists of a ten digit number. There are thus a possible 10^{10} different user identification numbers available for each system. As the system differentiates between Key card and IR-tag keys this number of possible combinations is therefore available on both technologies.

Please note that the reader operation is totally re-configurable, e.g. the ‘Open Door’ signal from the VISIKEY may not open the door, but may trigger a timer, to then allow the door to open after a period of time.

Obviously, other operations are possible. Please refer to Section 19 and Appendix 3 for further information.

Chapter Four

Computing Requirements

To operate, the VISIKEY requires the use of an IBM or compatible personal computer (PC) With Windows ™ installed. This computer, chosen because of its reliability, processes the information received from the remote card readers and then controls their operation. Instructions may be sent to allow or deny entry, or to trigger an alarm condition.

The computer continuously monitors the status of the entire system and displays this information in an easily assimilated form. Although designed to run without operator attention, any required information can be easily requested and rapidly displayed, allowing an operator to change the VISIKEY ‘s operational parameters instantly.

Computer specification

- P3 500Mhz Personal Computer or better.
- 100Mbyte free hard disc drive (larger drives permit larger history files).
- 1.44Mbyte 3.5" floppy disc drive (for installation).
- VGA interface card or higher (preferably with XGA driver).
- SVGA colour monitor or higher.
- XT/AT type keyboard.
- Mouse, trackerball, or other pointing device. (Microsoft Mouse compatible).

Chapter Five

Software Installation

To run the system, first install the Security Device. This device should be plugged into the Parallel Printer Port at the back of the PC. This device ***MUST ALWAYS*** be present whilst using the VISIKEY, else no communication to any serial COMMs or printer port is possible.

When an upgrade of software becomes available, the new installation will not cause the previous configuration to be lost. The old backup file will be accepted by the newer VISIKEY.

To carryout the installation/upgrade, place the VisiKey installation disc into the 'A' floppy drive select 'RUN' from the start menu computer. Type:

A: SETUP<Enter>

And follow the on-screen prompts.

Next insert the Hardware key driver installation disk into the 'A' floppy drive select 'RUN' from the start menu computer. Type:

A: DK2WIN32<Enter>

And follow the on-screen prompts.

After installation of the hardware key drivers your machine will reset. Once windows has reloaded run the VisiKey software which is located in the Morley folder in the Applications menu.

NOTE If you have requested a Desktop shortcut to VisiKey software use the shortcut only to run the software do not use the shortcut whilst the software is already in operation. If you require to maximise the software whilst in operation click on the key Icon located in the application tray.

Express Install

The VisiKey software includes an 'Express install feature which allows a initial system configuration to be carried out with limited system knowledge. This option is located in the 'Config' menu. Note that to obtain access to this menu option you must have set the password access rights to allow 'Config' access.

windows and pointers

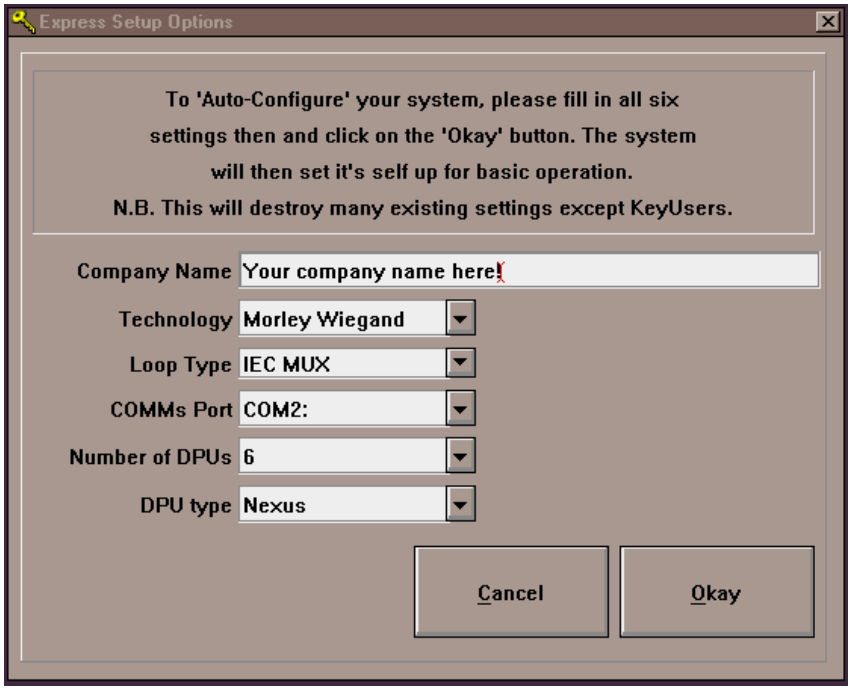


Fig. 5.1 Express installation dialog box

To carryout an express install first enter the end users company name in the box provided. Next select the reader technology type to be used on the system. If the system is an RS232 or RS485 based network the Loop Type should be set to ‘IEC MUX’. Determine which serial port you wish to use on the PC an select it in the ‘Comm Port’ selection box. Finaly select the number of controllers you wish to configure and the type of controllers being used. You are now ready to configure the system, depress the ‘Okay’ button, at this point you will be asked to verify the configuration, when complete the VisiKey software will restart. When the software has restarted it will function as a working system the only additional requirment to test the system will be the addition of a card user to the database.

Chapter Six

Changing Passwords

The password which allows full access to all operations is automatically defined when the software is first installed, to allow the system to be initially configured. The log in name is SUPERVISOR and the password is SYSTEM. It is recommended that the password be changed as soon as system access is gained. The log-in name SUPERVISOR can also be changed if required.

To enter the VISIKEY software you must first log-in. Click on the ‘LOGIN’ icon on the Icon Bar. A window will appear requesting name & password.

A thin, red, line will appear on the left-hand side of the ‘User Name’ box. This is the cursor. Now type:

SUPERVISOR <Enter>

The cursor will now be entered into the ‘Password’ box. The password will be displayed as asterisks (‘*’) for security. Now type:

SYSTEM <Enter>

You are now logged-on in the system.

If an error message appears simply click where indicated and try the procedure again, making sure of the correct spelling each time. The case of the letters (i.e. upper or lower case) is not important. If the password for Supervisor has already been changed or the user name of Supervisor has been modified, then consult the engineer who carried out these changes.

Once you are logged onto the system, select ‘SYSTEM’ on the Icon Bar. A menu will now pop up (Fig 8.1). Select the ‘Passwords’ option, then a window displaying user names and passwords should now be displayed (Fig 7.1). A number of blank boxes will be present below the user name / Password bars denoting levels of access. Clicking on any of these boxes will allow access to that level. These boxes toggle on/off by clicking on them blank is off red is on. Click on all buttons to gain full access to the system and then close the window

To change the supervisor password select 'LOGOUT' as described earlier. Then select the 'change password' option. a window will appear requesting the current password therefore type:

SYSTEM <**Enter**>

The cursor is then entered into the 'New password' box below. Type the new six character password and verify in the box below. Thus the supervisor password is now changed.

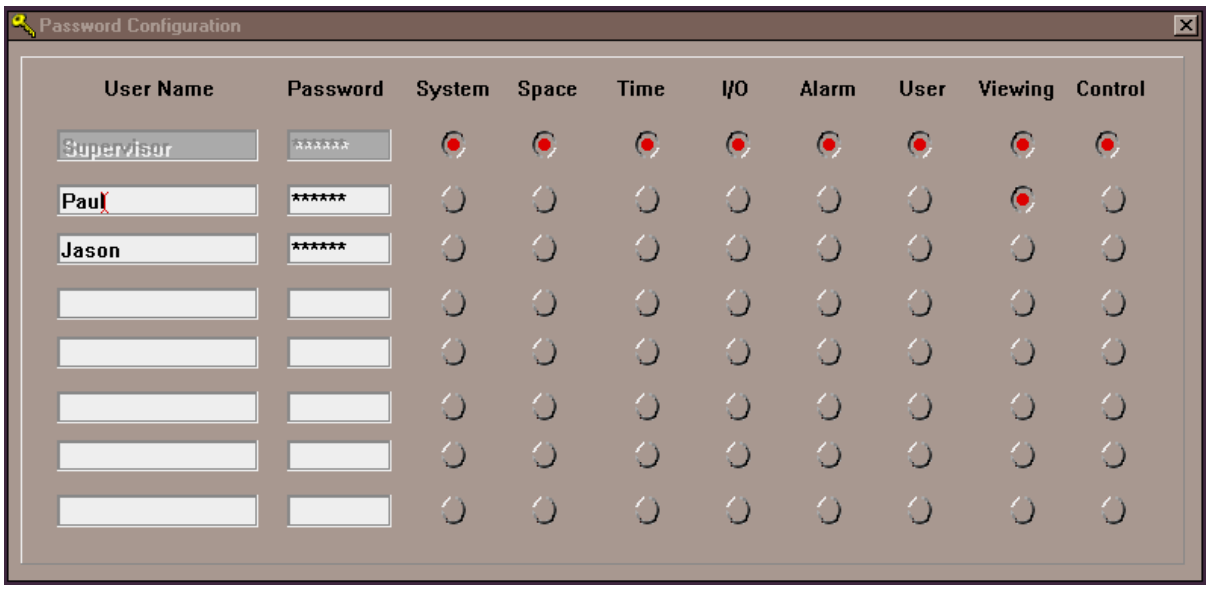


Fig. 7.1 The System Password Configuration Menu

Chapter Seven

The System Menu

Fig. 8.1 The SYSTEM menu.

Who is Logged On?

This displays which console operator is logged onto each terminal (on a Multi-User System) and at what time they logged in. This is updated in real time.

Enabling Other Operators

Once the Supervisor log-in name and password have been selected then the access rights of other operators of the system software can be defined. More than one operator can have full access rights if necessary. This section will tell you how to enter the user-names of other users, their passwords and how to define the access rights that they have.

It is recommended that more than one person has access to the full range of system rights in case of sickness or accident. This could be done simply by having two people log in as the same person i.e. as SUPERVISOR, with the appropriate password (which you should have changed!). This, however, will not allow you to distinguish between these persons on the security record. It is therefore recommended that these two persons have entirely separate user names and passwords. Passwords should, of course, be kept secret. The more widely that passwords and their associated user names become known, then the greater the risk to system security. Two persons should not have the same user-name.

Once you have decided on the rights for the other operators of the system, return to the 'Password' window by selecting the 'System Menu' and then selecting 'Passwords' on the menu. Now you can enter the names of the other system operators and their access rights.

Click on the left-hand side, in the column entitled 'User name'. The cursor will appear. Make sure that this cursor is at the far left-hand side of the box, either by clicking with the mouse pointer there, or by moving it there from the keyboard, using the arrow keys. Now enter the user name followed by **<Enter>**. Now move across to the box on the right-hand side in the 'Password' column and enter the operators password. Press **<Enter>** again. Another operator has been added to the system. Repeat this process as many times as is necessary (up to eight times).

Operators may be allowed to choose their own passwords, but they should keep these secret. Only the specific operator and persons with 'System' access should know other operators passwords. Passwords should not be anything obvious e.g. a wife, son or daughters name, or a telephone number. Easily guessed passwords like these can threaten system security. A good way to choose passwords is to randomly open a dictionary and choose the first word of at least six letters on that page. Thus, the password choosing process is randomised and unauthorised tampering with the system made much more difficult.

Quit

This option returns program control back to the shell that launched the VISIKEY. It is not recommended that the computer controlling the VISIKEY is used for other tasks as this could lead to compromises in building access control and security. The system will place all readers into standalone mode if this option is chosen.

Restart

Restarts the VISIKEY. All system files are saved, ready to be re-loaded. This is useful if the configuration of the system has been changed, and will not take effect until the system is restarted. The system will place all readers into standalone mode for the duration of shutting down the system and restarting if this option is chosen.

Shut Down

This will save all data and close the system down. One window will be displayed, prompting the operator to restart the system - when appropriate. The system will place all readers into standalone mode if this option is chosen. This function may be carried out automatically when a critical situation arises, such as the loss of mains power and a low UPS battery; although this is fully configurable in the *Environment* window.

Environment

Allows the setting of time, time zoning, daylight saving date and times, screen saving, auto logout, auto shutdown, backing-up time, backing-up to floppy disc, screen display layout and the setting of the company name.

the system menu

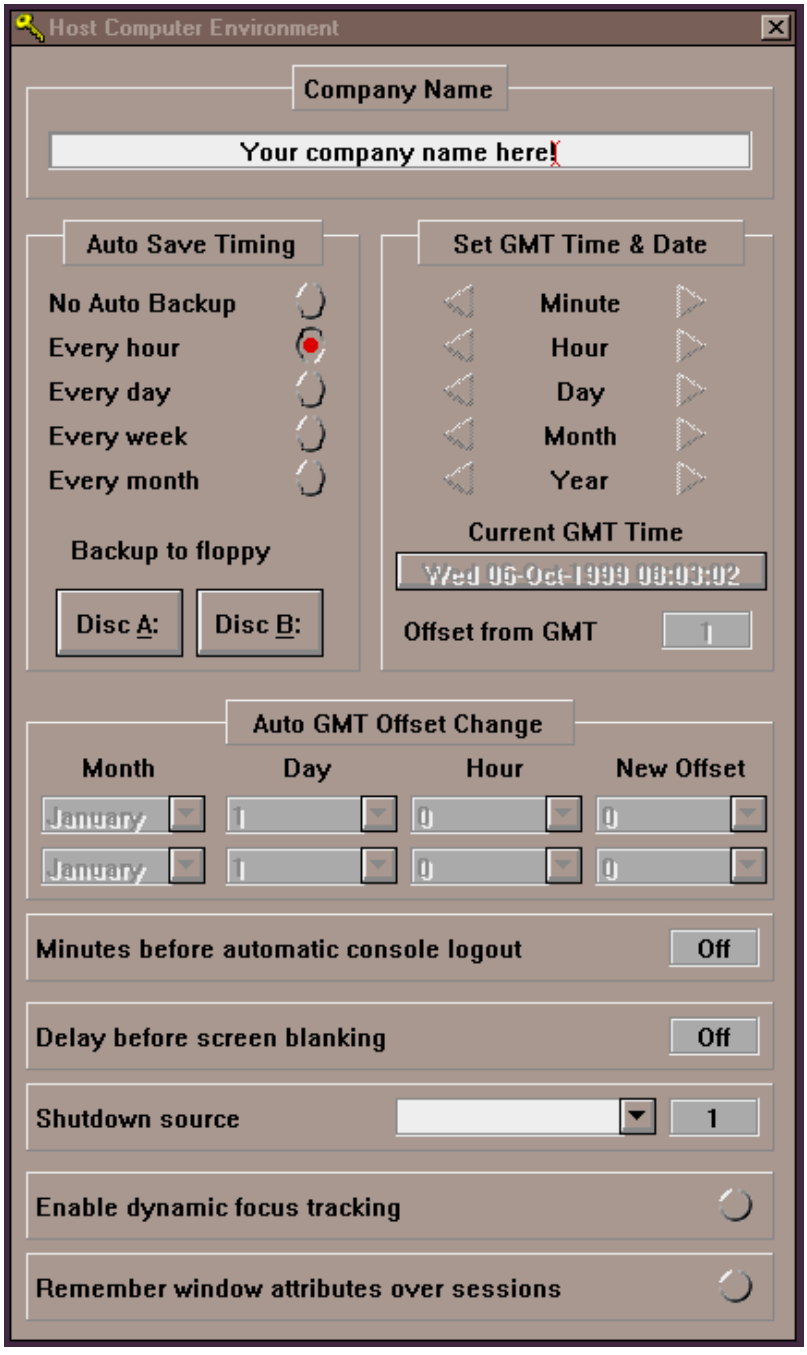


Fig. 8.3 The Environment Window.

- Once the system is installed, the correct time and date will be obtained from Windows ™ .
- The screen may be switched off and the operator may be logged out after a predetermined period of time with no use. The former preserves the screen (prevents *burn-in*) and the latter preserves system integrity.

- The system may be automatically shut down by setting a reader and alarm condition to source this procedure. This could be a CCM unit (Contact Condition Monitor) connected to an UPS (Uninterruptable Power Supply) mains failure output.

- The 'backing-up time' option sets the frequency with which the system automatically writes a copy of its current files onto the hard drive. This is a precautionary measure against complete power failure or any other event which may cause the computer memory to be wiped or otherwise disrupted. It is an important option and its use should be carefully considered. It is rarely necessary to make a back-up copy of the system records every minute, a back-up time of once a day should prove sufficient for most users. Remember, the more often the system records are backed-up, the less data will be lost if there is a disruption.

- Backing-up to floppy disc is carried out by clicking on one of two buttons, marked 'A:' and 'B:', representing the two possible floppy drives on the host computer. To backup, place a *formatted* disc into the required drive and clock on the drive button. The backup shall take place. On completion simply remove the disc and store it in a safe place. If during a backup, a textual message appears explaining a disc error, then refer to your Windows help about which action you should take. Please note that whilst this error is displayed and the system is awaiting your response, the VISIKEY has ceased operation temporarily.

- The company name, as set by the user is continuously displayed in the bottom left-hand corner of the screen whilst the system is in operation, unless it is covered by an active window.

Force Backup

This forces a backup of the entire system set-up and Keycard Holders to the hard drive. This should be used on a regular basis when entering lots of information into the VISIKEY, to ensure a copy is stored away. The timed backup carries out the same function but on defined time periods.

Chapter Eight

The CONFIG Menu

The options available from this menu allow the custom configuration of the system to the users requirements. The setting of these should be carefully considered. Before using these options you should consult the manual Chapter 15, ‘Planning Your System’.

Day Types

There are 32 different Day Types which are user defined. Each Day Type can have up to eight start/stop time ranges included in it. Each Day Type is labeled with a particular name of the operators choosing. As an example, a Day Type which allowed access from 8-45 a.m. to 5-30 p.m. could be labeled ‘Normal Day’, a Day Type that allowed no access could be labeled ‘No Access’. Each Day Type is also allocated a particular label by which it is addressed e.g. ‘Normal Day’.

Week Types

There are 32 different Week Types which are user defined. Each Week Type consists of a list of seven Day Types, entered by the operator and addressed by their previously assigned labels. e.g. ‘Normal Day’ or ‘No Access’. A typical Week Type might consist of two ‘No Access’ days and five ‘Normal Days’. A Week Type of this sort might well cover the majority of the employees within a company, and still leave another 31 Week Types free for more specialised uses. Each Week Type is also allocated a particular label by which it is addressed e.g. ‘Normal Week’.

Year Types

There are 32 different Year Types which are user defined. Each Year Type consists of a list of 53 Week Types, entered by the operator and addressed by their previously assigned labels. e.g. ‘Normal Week’ or ‘No Access’. A typical Year Type may consist of 53 weeks of ‘Normal Week’ giving normal access throughout the year. Once one or more entries are entered into a Year Type window, they may be replicated throughout the year. The replication step allows the easy definition of shift working etc. e.g. A pattern of ‘Night Shift’ and ‘Fore Shift’ on alternate weeks. Each Year Type is also allocated a particular label by which it is addressed e.g. ‘Normal Year’.

Holidays

This option allows the setting of holiday information by date. It sets ‘Global Area’ departmental access overrides on these chosen dates. For example, if a date is specified as a holiday, then only those persons in the Security or Maintenance departments might be allowed into the building.

Departments

This allows the setting of department names e.g. Security, Management, Engineering etc. and defines the limits and times of access for these departments into Areas through the relevant Access Rights window. See Chapter 14.5, ‘Defining Departments and Their Access Rights’.

the config menu

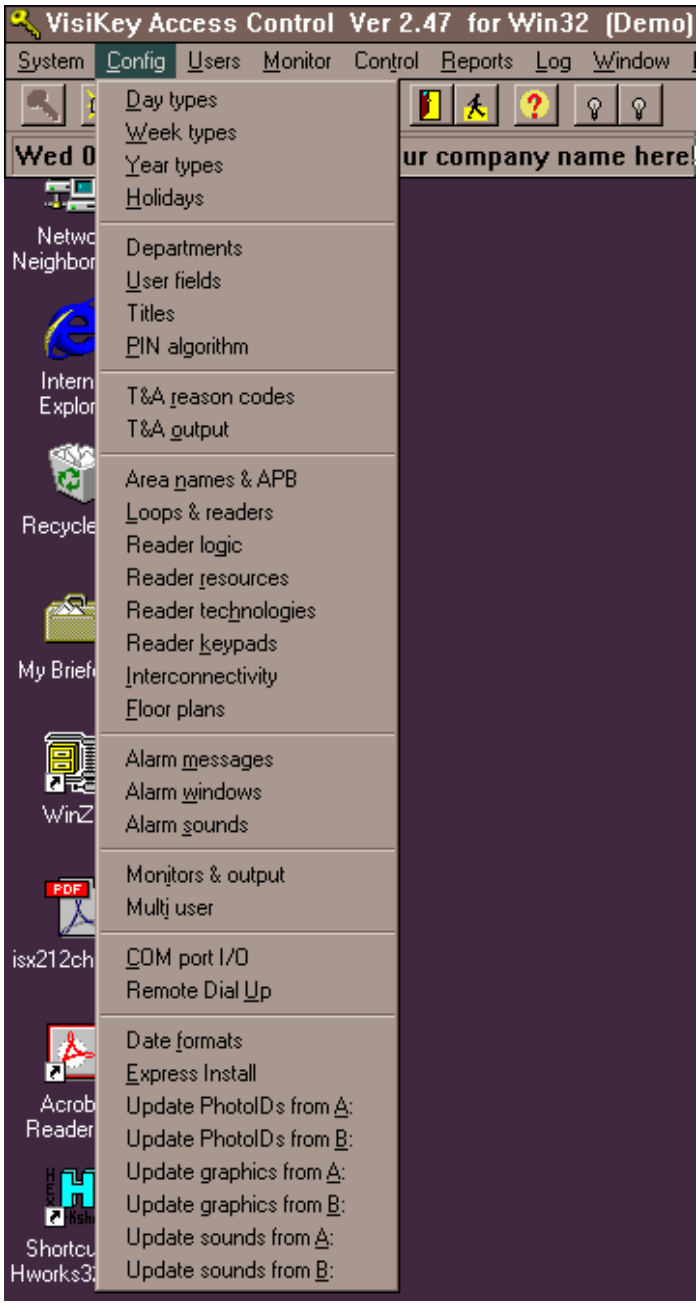


Fig. 9.1 The CONFIG menu.

the config menu

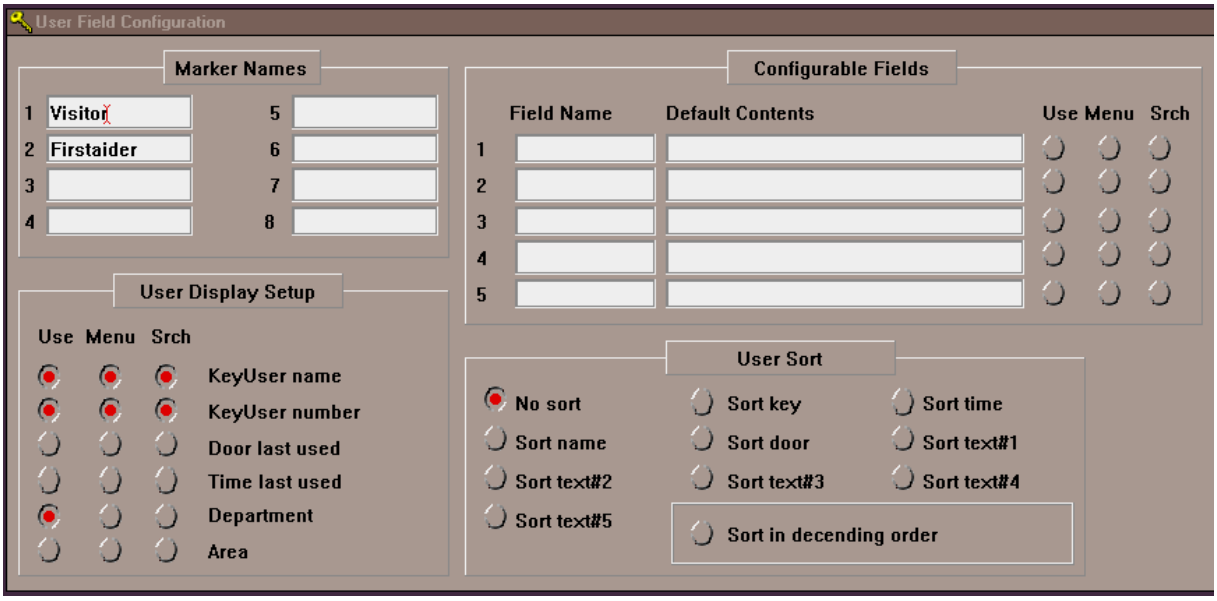


Fig. 9.2 The User Field Configuration.

User Fields (see fig. 9.2)

Permits the configuration of user fields, both text and logical. These fields are used in the Create Users option and allow the custom configuration of user information. See Section 14.5 for more detail.

Titles

Allows the configuration of titles in the 'Titles' window which will appear when new Keycard Holders are added to the system. Simply click on an empty bar and type in the new title. To alter a title, simply click on the bar you wish to change and alter the entry as appropriate.

PIN Algorithm

When used with the Auto-pin option on the Create User window, this allows PINs for employees to be automatically set, thus saving time and effort.

A four figure number is entered in the PIN Algorithm box. When the Auto Pin option is utilised later, the PIN Algorithm number is multiplied, without carry, with the lowest four digits of the users Key number. This number is then the users PIN. For example:

PIN Algorithm number : 4735

New users key number: 9876543213

Now, 4x3=12, but there is no carry, so =2.

7x2=14 but there is no carry, so =4.

the config menu

3x1=3

5x3=15 but there is no carry, so =5.

Therefore, the auto-PIN, as assigned to the user by the VISIKEY is 2435. The PIN Algorithm number need only be set once for all users. This feature massively simplifies the task of issuing PINs. The calculated auto-pin is automatically entered into the appropriate section on the New User window

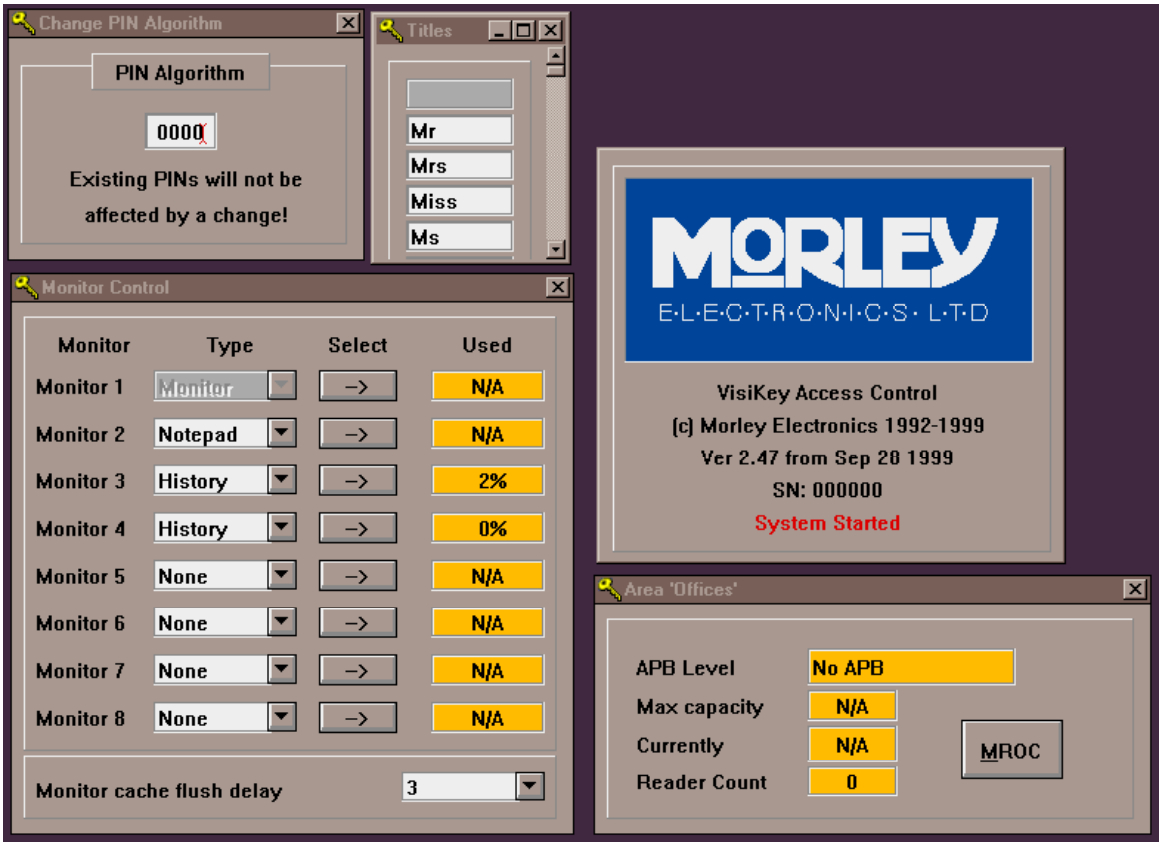


Fig. 9.3 Title, PIN Algorithm, Monitor Control and Capacities Windows.

the config menu

Time & Attendance Reason Codes

Time & Attendance Reason Codes allow the setting of valid numbers which may be entered at T&A Enquiry reader. It is essentially a validation system. Note that the first two entries are fixed and are sent on a T&A In and Out respectively.

Time & Attendance Output

This sets the output format of T&A information. It permits the setting of which users fields are assembled into a T&A record.

Area Names, APB and Capacity

(See Fig 9.4)

Allows the naming of areas so that other parts of the VISIKEY can address them by this name, rather than just a number. A group of readers could be assigned a name such as 'Laboratory'.

The Anti-Passback (APB) level of the Area can also be set. Someone wishing to enter a level with a certain anti-Passback value must also have been recorded by the system as entering all levels with a lower APB value. APB is set by defining which area the current area resides (e.g. The *Stores* area may be within the *Admin* area).

A person cannot re-enter a certain APB level without first having left it. This prevents card lending between employees. An Area with an APB level set must therefore have one or more in and out readers so that the VISIKEY can monitor both entries and exits of personnel.

An Area with an APB level can also be set with a maximum capacity limit if required. Once this limit is reached, no more persons will be admitted until someone has left.

There can be up to 128 areas.

Capacity List

Allows the setting of capacities in the 'Capacities' menu, which will appear when selected through the option above, for setting Area capacities.

Loops and Readers

(See Fig 9.6)

The initial window allows the definition of loop names for a specified group of DPUs and the setting of which loop is controlled by which COMMs port.

From the Loops window, further loop dependant windows contain information about individual DPUs on a loop such as the readers Technology (Card or IR-tag etc.), Logic Type (how a reader operates), Reader Type (APB type etc.), the Area in which it resides, the ISO Track/Read direction, resource specification and the number of reader heads the DPU supports.

the config menu

Reader Logic

Allows setting of names for logic type and entry/editing of DPU scripts. For more information see Chapter 16, ‘Programming a Reader’.

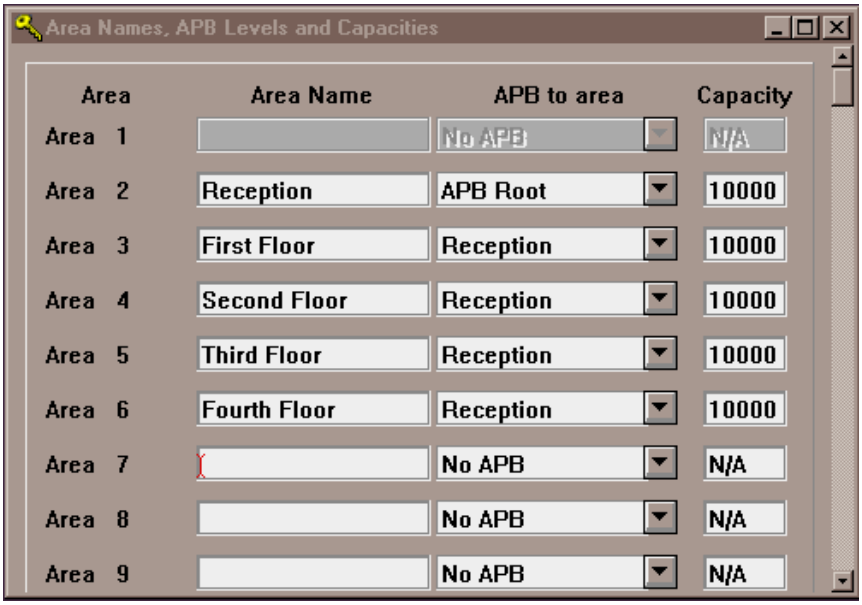


Fig. 9.4 The Area Names and APB window.

Reader Resources

The reader resources allow configuration of which physical inputs and outputs are used by each *reader* within a DPU. By default readers have 2 CCM inputs and 2 relay outputs. This is totally soft configurable and permits systems with up to 16000 inputs and 16000 outputs on the same DPU.

Reader Keypad Layouts

This permits the setting up of keypad layouts on Morley type DPUs for non-standard keypads. The function of each key may be defined by the user to allow keypads to be mapped in any way.

Reader Technologies

The defining of reader technologies is a complex but extremely flexible way of allowing new card technologies and formats to be used on the VISIKEY software with Morley DPUs. For each technology the hardware interface type may be defined (Watermark, Wiegand and SoftMagnetic), whether it has one display LED or two, whether bi-directional reads are permitted, whether sentinel data ought to be searched for within a data stream, the bit pattern of a data stream (data, sentinel and check bits) and the resultant number format.

the config menu

The system as default has a number predefined reader technologies, standard and LRC Watermark, Wiegand-24bit Hex and Wiegand-24bit BCD.

Interconnectivity

This allows system variables to be processed and then made accessible to all DPUs on the system. For example, a flag indicating that no-one is left within a building so the lights may be turned off! This information would be sent to *ALL* DPUs and they may take action accordingly.

Codes for Global Scripts

area_count <area_num>

ccm_state <loop> <reader> <head> <ccm_num>

alarm_state <loop> <reader> <head> <alarm_num>

var_state <var_num>

These may be used in global scripts (Interconnectivity) in such examples as below:-

area_count 3 < 2

This means the statement is true when the count of people in an area (must be APB area) is less than 2.....

Floor Plans

Allows the setting of up to 32 floor plan textual descriptions and the filename of the plan file.

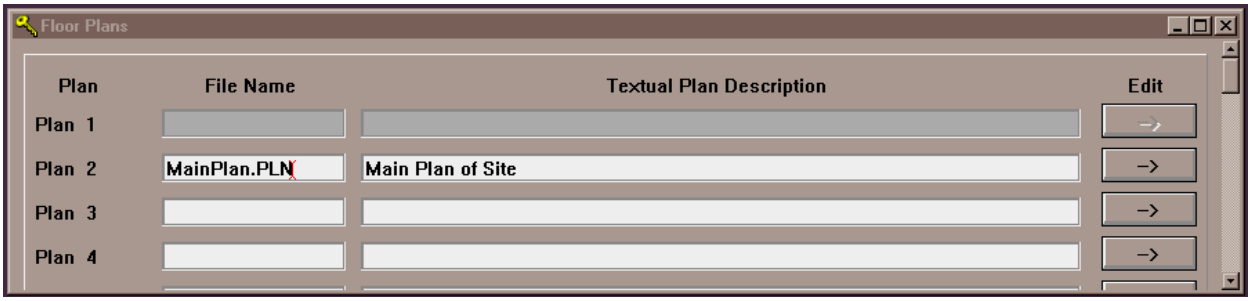


Fig. 9.5 Floor Plans window.

the config menu

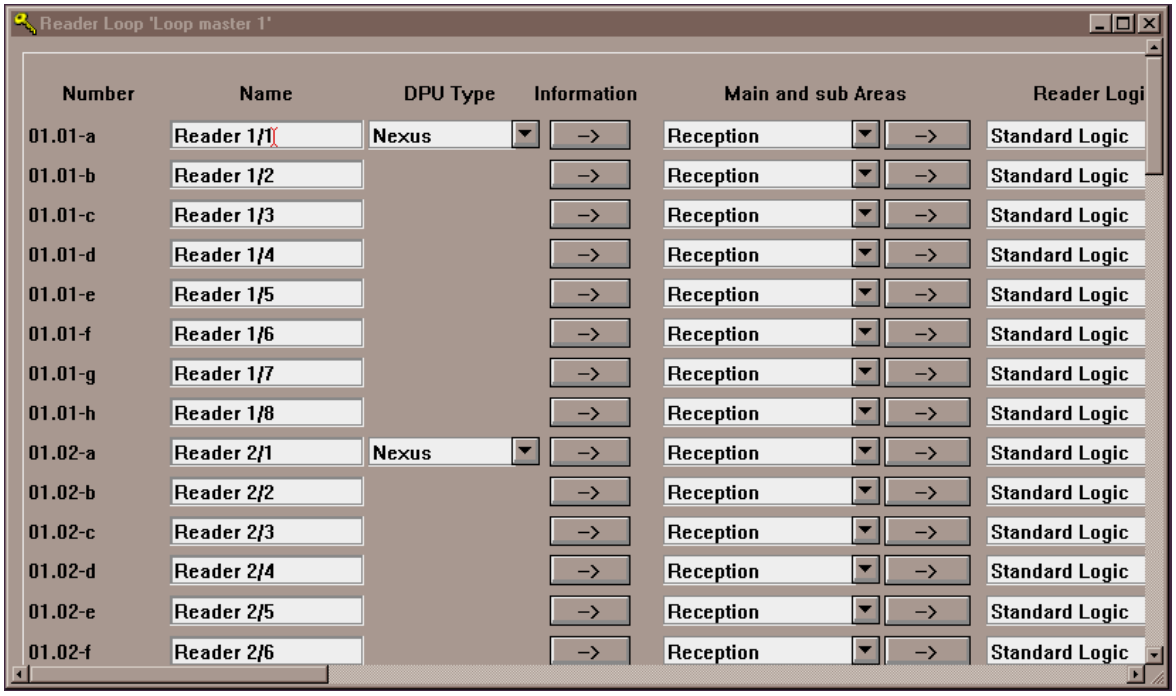

Reader Loop 'Loop master 1'
Number
Name
DPU Type
Information
Main and sub Areas
Reader Logi
01.01-a Reader 1/1 Nexus -> Reception -> Standard Logic
01.01-b Reader 1/2 -> Reception -> Standard Logic
01.01-c Reader 1/3 -> Reception -> Standard Logic
01.01-d Reader 1/4 -> Reception -> Standard Logic
01.01-e Reader 1/5 -> Reception -> Standard Logic
01.01-f Reader 1/6 -> Reception -> Standard Logic
01.01-g Reader 1/7 -> Reception -> Standard Logic
01.01-h Reader 1/8 -> Reception -> Standard Logic
01.02-a Reader 2/1 Nexus -> Reception -> Standard Logic
01.02-b Reader 2/2 -> Reception -> Standard Logic
01.02-c Reader 2/3 -> Reception -> Standard Logic
01.02-d Reader 2/4 -> Reception -> Standard Logic
01.02-e Reader 2/5 -> Reception -> Standard Logic
01.02-f Reader 2/6 -> Reception -> Standard Logic

Fig. 9.6 Readers within a loop.

Alarm Messages

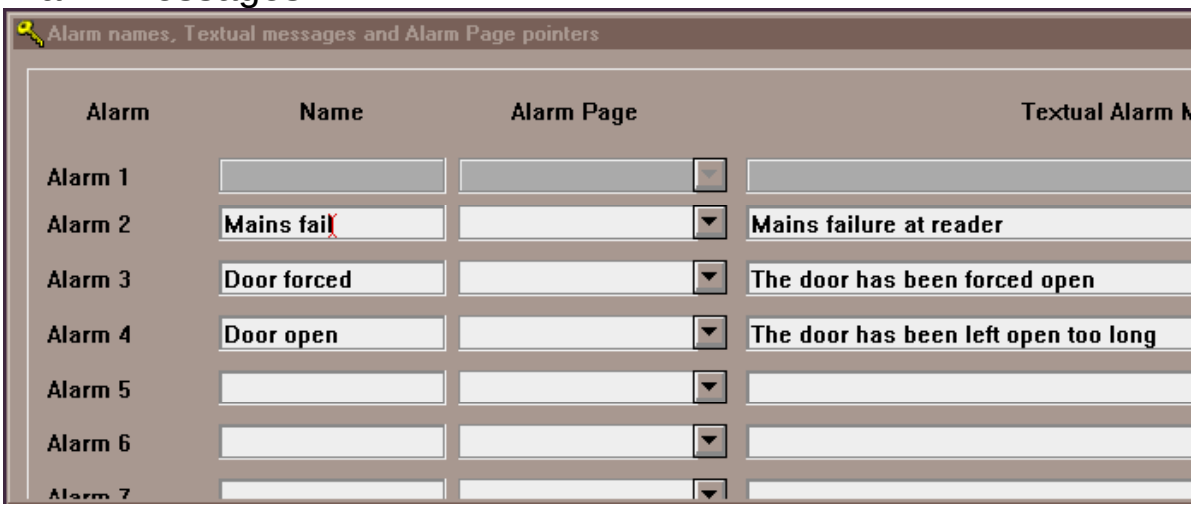

Alarm names, Textual messages and Alarm Page pointers
Alarm
Name
Alarm Page
Textual Alarm M
Alarm 1
Alarm 2 Mains fail Mains failure at reader
Alarm 3 Door forced The door has been forced open
Alarm 4 Door open The door has been left open too long
Alarm 5
Alarm 6

Fig 9.7 Alarm Messages Window

Allows the setting of the text of up to 255 alarm messages and names. When an alarm is signalled by a reader its type is decoded by the VISIKEY and then the relevant alarm

message can be displayed. This window allows you to set the text that will appear when any given alarm is notified to the system.

Each alarm message may also point to an ‘ALARM WINDOW’ or ‘PAGE’ which is a separate window on the screen, describing the alarm condition in detail. For more information about alarms see the Chapter 16, ‘Programming a Reader’.

Alarm Windows

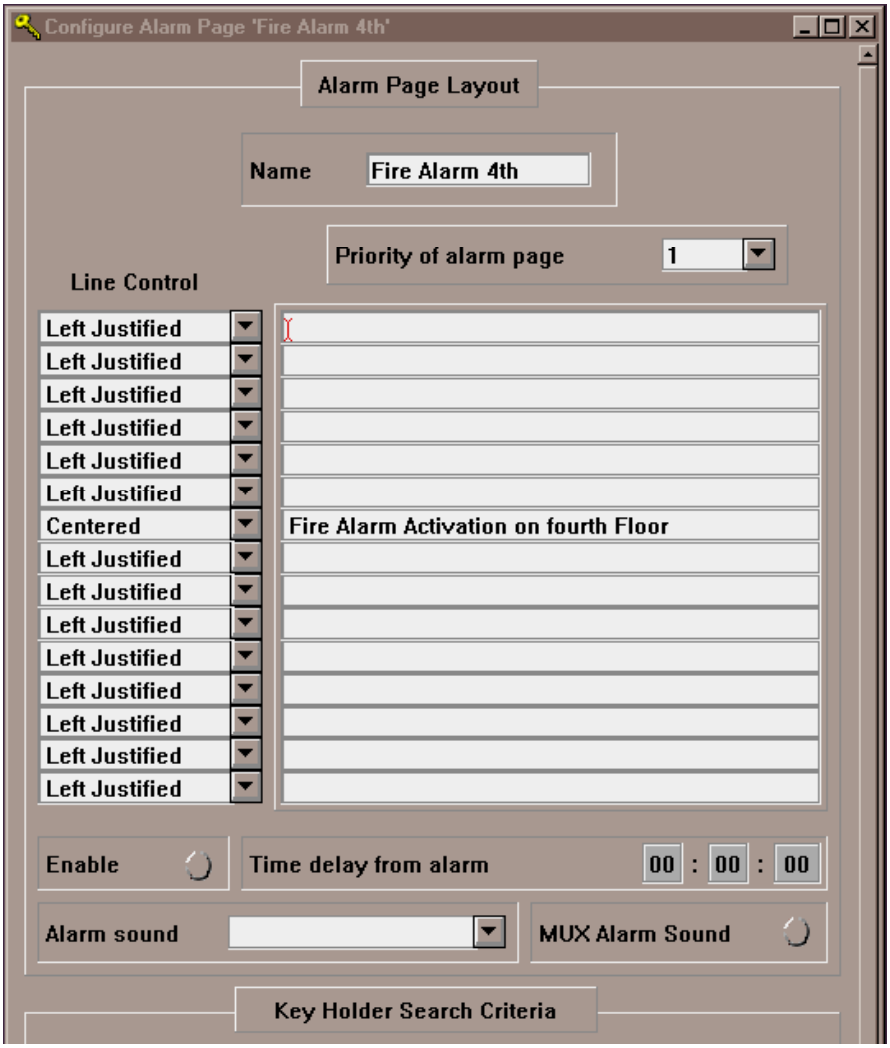


Fig. 9.8 An Alarm Window definition.

An Alarm Window is a custom screen which will appear under a predetermined circumstance, of which the layout is defined here. The priority sets the importance of the window; the lower the number, the greater the importance. If a greater priority window wishes to appear when a lower priority window is already shown, then the former window is pushed onto a stack, and the latter window shown. The stack has a depth of 64 windows. Two sets of operations may

be carried out by this system, the actual displaying of a defined window and a Muster. Both can be individually enabled to allow one or both to be activated.

Each of the 15 lines of the window may contain up to 40 characters, which can be left, right or centrally justified using the justification option to the left of each line. The time delay for a window, shown below the window definition, is the time before the window is displayed.

An audible sound can be programmed to occur when an Alarm Window is activated. This is done by selecting a sound from the pre-programmed library.

A 'Muster Dump' may also be activated by an alarm. This is defined by the lower section of the Alarm Window definition window. The options are of an 'AND' nature with all Keycard Holders found being displayed on all configured 'USER SEARCH' output devices (i.e. printer).

Alarm Sounds

(See Fig 9.9)

All sounds in the VISIKEY are configurable. The parameters for each of the 31 different sounds (the first sound is permanently set to silence!) include initial pitch, pitch step, pitch step rate (in 53ms steps) and duration (also in 53ms steps).

The initial pitch is in the range of 0 to 16383, which covers most of the humanly audible spectrum, with 0 being the lowest frequency. The pitch step is also in the range of 0 to 16383.

The pitch step rate is a temporal distance between each pitch step. This is counted in 53ms steps (1/18.2th of a second). The overall duration of the sound is also in defined in multiples of 53ms.

the config menu

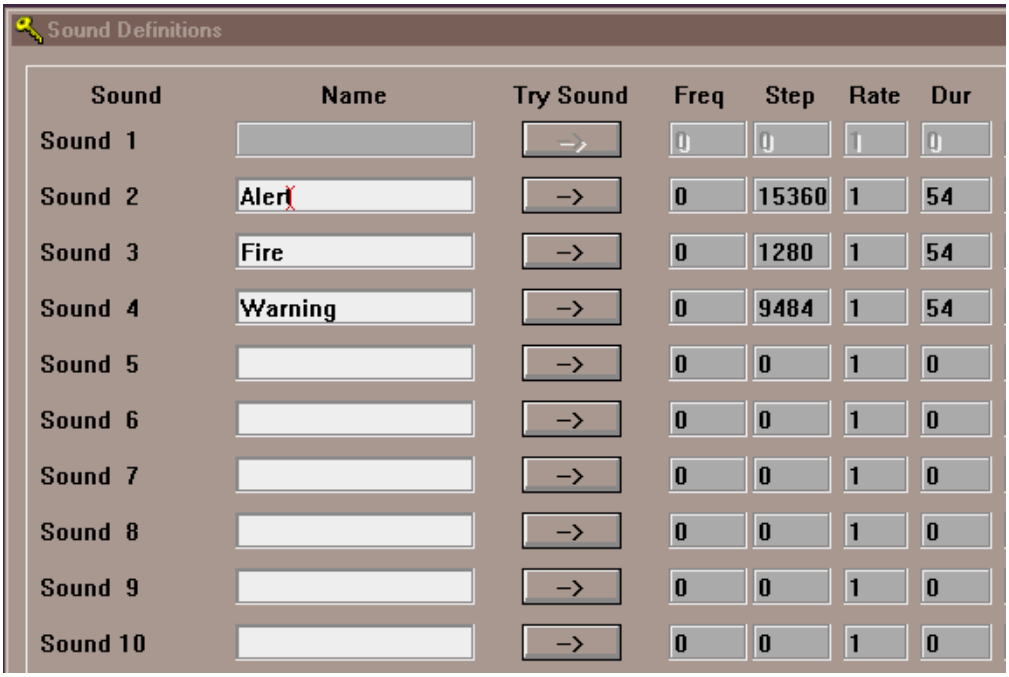


Fig. 9.9 The Sound definition library.

Monitors and Outputs

Allows the setting of up to eight output devices for the printing and/or logging of all, or any combination of VISIKEY monitor registering operations. Files, MDA-type (i.e. monochrome) monitors, COMM ports and windows can all be addressed individually by the VISIKEY and any combination of monitor information sent to each. e.g. all types of monitor information could be sent to a file on a remote computer via the COMMs link, for added security.

History files are created from this option. The operator must specify the size (in total number of single line entries) and name of the file (in DOS filename restriction format) and select the 'CREATE' button. The VISIKEY will create the file, but will truncate it if insufficient disc space if available.

See Section 10, 'The MONITOR Option'.

COMMs Port I/O

(See Fig 9.10) The COMMs Port I/O window allows the I/O (Input/Output) port address and IRQ (Interrupt Request) vectors to be set for interface cards. The entries instruct the VISIKEY as to where the specific address of such I/O devices is to be found and how to signal to the device that it is ready to communicate monitored information.

For each COMMs port, the baud rate, number of data bits, number of stop bits, parity type, handshaking type and which terminal (Host or Slave on Multi-User Systems) must be specified. The settings should correspond to the device to which it connects, therefore it is prudent to consult the manual or documentation supplied with the devices.

the config menu

The connection to a 485 Loop driver is as follows:

- 9600 baud
- 7 bits
- 2 stop bits
- Even parity
- DO NOT use CTS/RTS
- DO NOT use XON/XOFF
- DO NOT use TIME-OUT

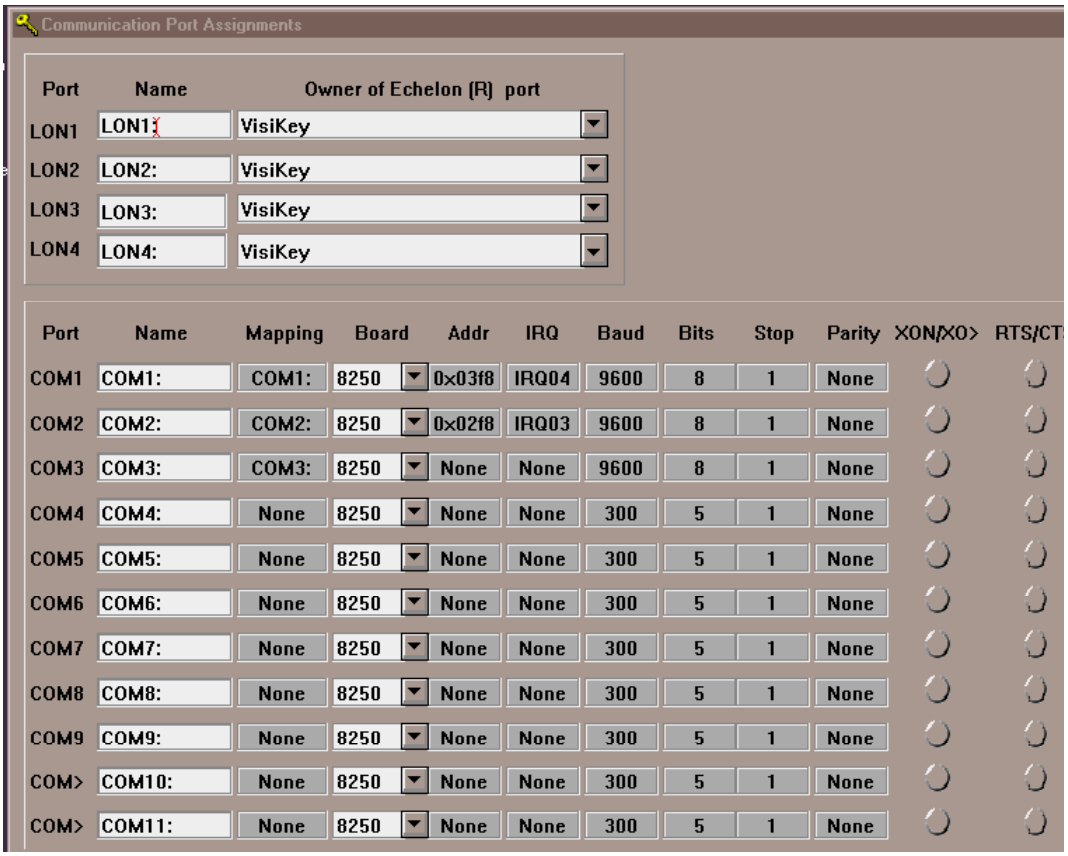

Communication Port Assignments
Port Name Owner of Echelon (R) port
LON1 LON1: VisiKey
LON2 LON2: VisiKey
LON3 LON3: VisiKey
LON4 LON4: VisiKey
Port Name Mapping Board Addr IRQ Baud Bits Stop Parity XON/XO> RTS/CT
COM1 COM1: COM1: 8250 0x03f8 IRQ04 9600 8 1 None
COM2 COM2: COM2: 8250 0x02f8 IRQ03 9600 8 1 None
COM3 COM3: COM3: 8250 None None 9600 8 1 None
COM4 COM4: None 8250 None None 300 5 1 None
COM5 COM5: None 8250 None None 300 5 1 None
COM6 COM6: None 8250 None None 300 5 1 None
COM7 COM7: None 8250 None None 300 5 1 None
COM8 COM8: None 8250 None None 300 5 1 None
COM9 COM9: None 8250 None None 300 5 1 None
COM> COM10: None 8250 None None 300 5 1 None
COM> COM11: None 8250 None None 300 5 1 None

Fig. 9.10 The COMMs Port I/O window.

Sub-area configuration

This option is available to the Morley DPUs and allows up to 16 sub-areas to be specified from within a main area via a keypad. The 'SUB AREAS' option is present within 'LOOPS & READERS ' at any reader configured as an ISC DPU. Clicking on the 'SUB AREAS' option

box at the bottom right of the ' READER LOOP ' window (See Fig 9.11) brings up the window shown in (Fig 9.12) in which 16 areas can be allocated to corresponding keypad buttons labeled '0' to 'F'. Note. these sub areas must be entered earlier in the ' AREA NAMES & APB' option in the CONFIG menu. Once configured the user will be marked into the area assigned to the button depressed.

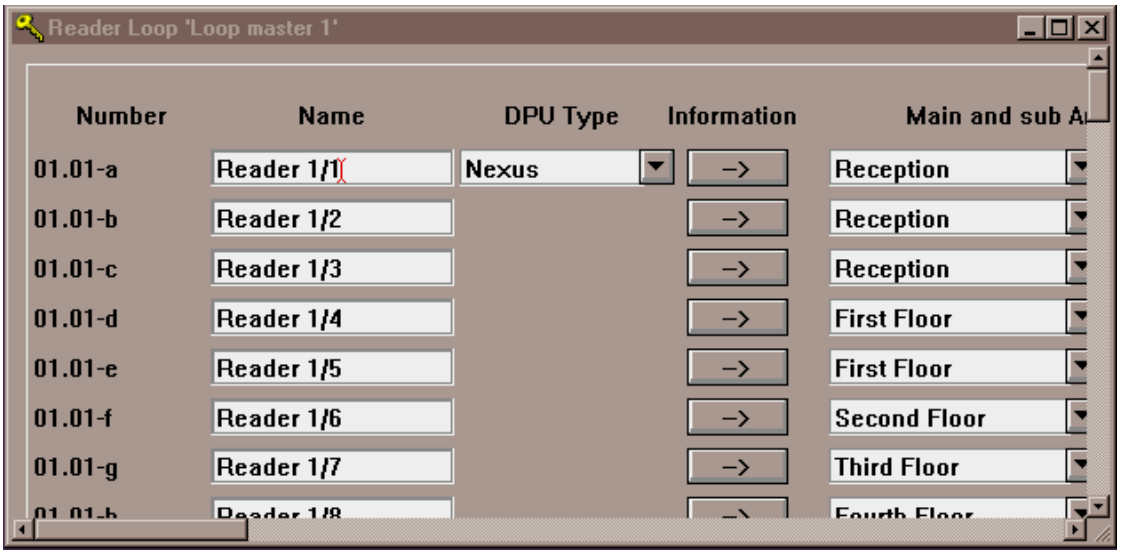


Fig 9.11 Reader configuration window

the config menu

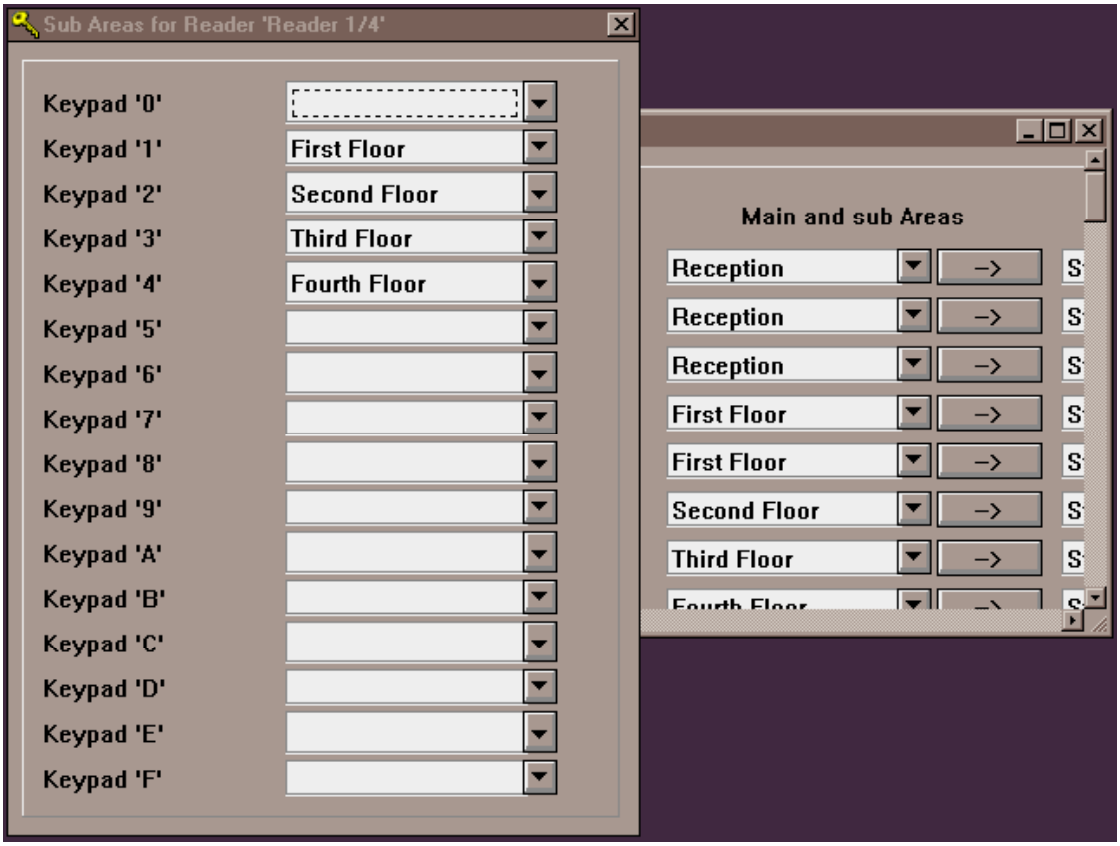


Fig 9.12 Sub-Area configuration window

Chapter Nine

USERS Menu

Create User(s)

Allows the creation of one or more Keycard Holders. Simply fill in the relevant fields and select Accept. The process is described in more detail in Chapter 14, ‘Entering a New User’.

Find User

(See Fig 10.1)This option allows the VISIKEY to search for Keycard Holders, using various textual labels, including wild cards. The operator could search for all those people in a building who were qualified as, say, first-aiders. The search categories into which a Keycard Holder is set are entered in the Create User option above. Each user can have up to eight yes/no pieces of information stored about them e.g. are they a first-aider? A search can also be for any other piece of information held about the user e.g. a search by surname, or even, by using a wild card, a search for all persons with surnames beginning with P, for example.

Output can also be sent to a configurable output device (e.g. a printer), if required. But the first 500 entries found will be displayed in the ‘FOUND KEY USERS’ window when the ‘FOUND’ button is clicked (See Fig 10.2).

Pack User Base

Compresses the user base, weeding out all those persons marked for deletion. This option, when utilised, allows faster processing of further requests on large, heavily used, systems.

users menu

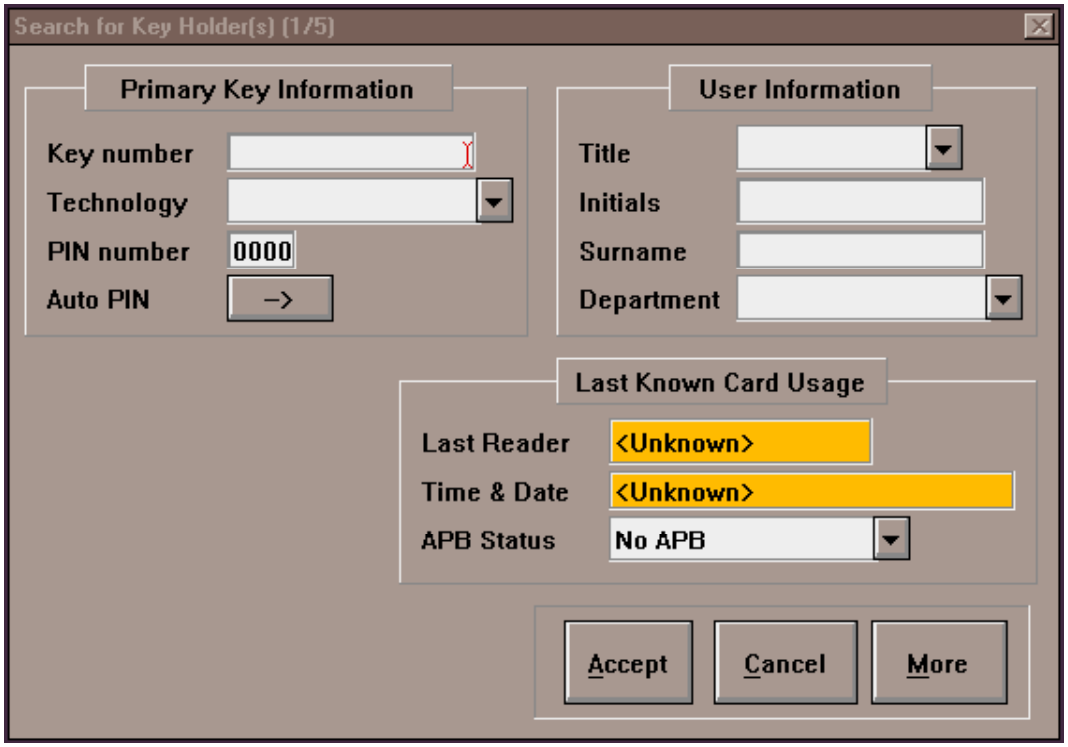


Fig. 10.1 The Search window.

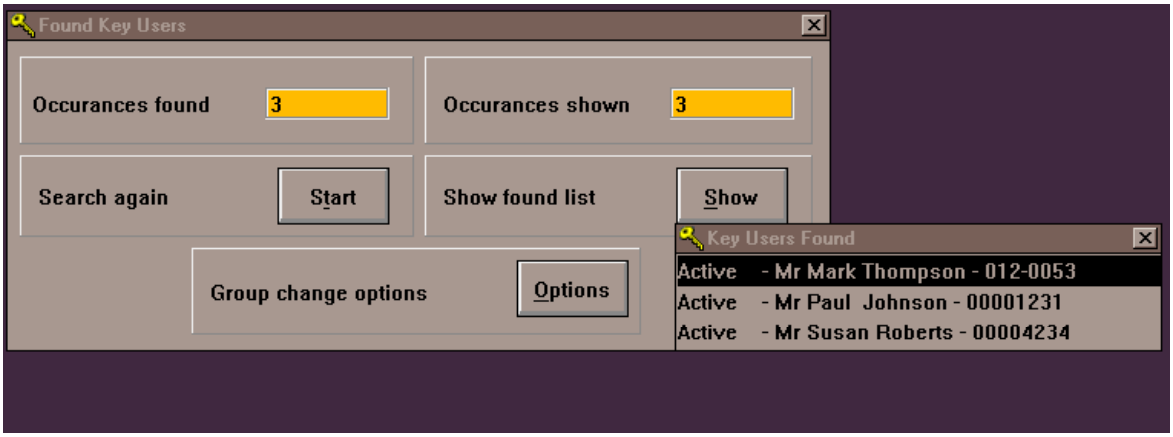


Fig. 10.2 Search Results.

Group user changes

This option allows a group of users with one or more common attributes to be modified on a group basis .e.g.. If all visitors cards were to be disabled at the end of each day, the operator could carry out a user search and using 'Group changes' disable all visitors cards.

users menu

This is achieved by use of a search in the 'FIND USER' option to specify the 'group' of Keycard holders that require modification.

As another example consider Fig's 10.3 to 10.6 .Suppose the 'repair' department was to become defunct and its Keycard holders were to be moved into the 'production' department. Using the 'FIND USER' option on the 'KEY USER BASE' menu a search would be carried out for the 'repair ' departments key holders. I.e. Enter the 'REPAIR' option from the drop down menu on the grey 'DEPARTMENT' box (Fig 10.3) and click on 'ACCEPT' to start search. A window titled ' FOUND KEY USERS ' will appear indicating the number of key users found (Fig 10.4) .Clicking on the 'GROUP CHANGE OPTIONS' will then bring up the window shown in Fig 10.5. From the drop down menu on the department box enter the 'PRODUCTION' option .Then enable this by clicking the white box to the ON state and clicking the grey change button on the bottom left of the window. The Keycard holders that were allocated to the repair department should now be in the production department

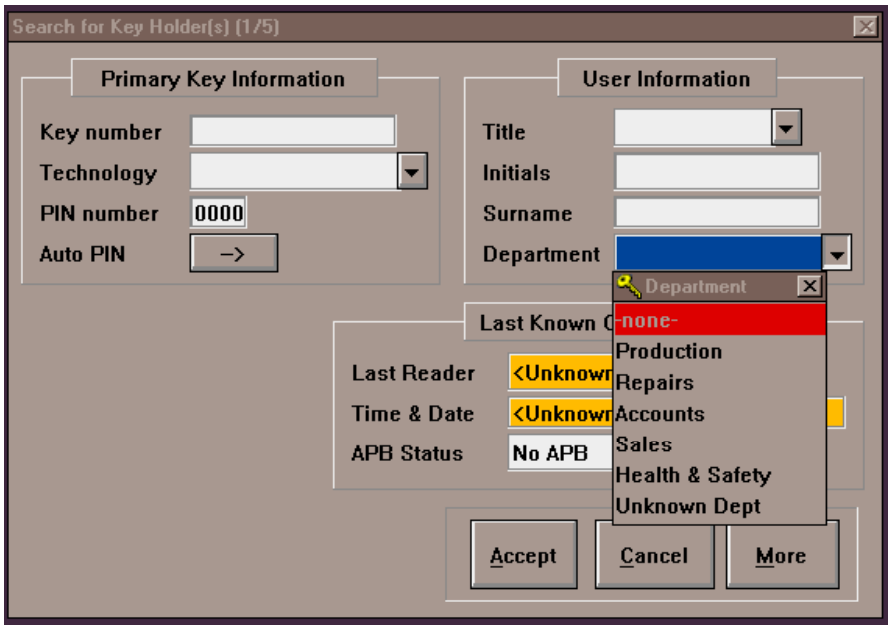


Fig 10.3 User search window

users menu

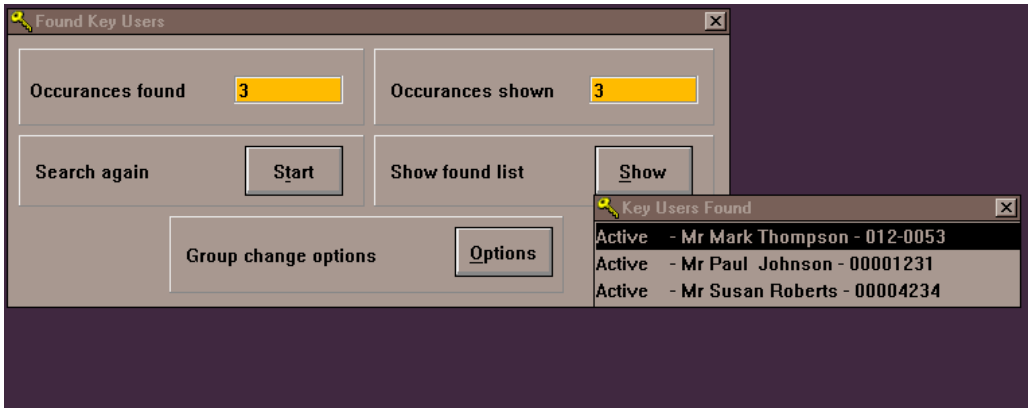


Fig10.4 Search Result window

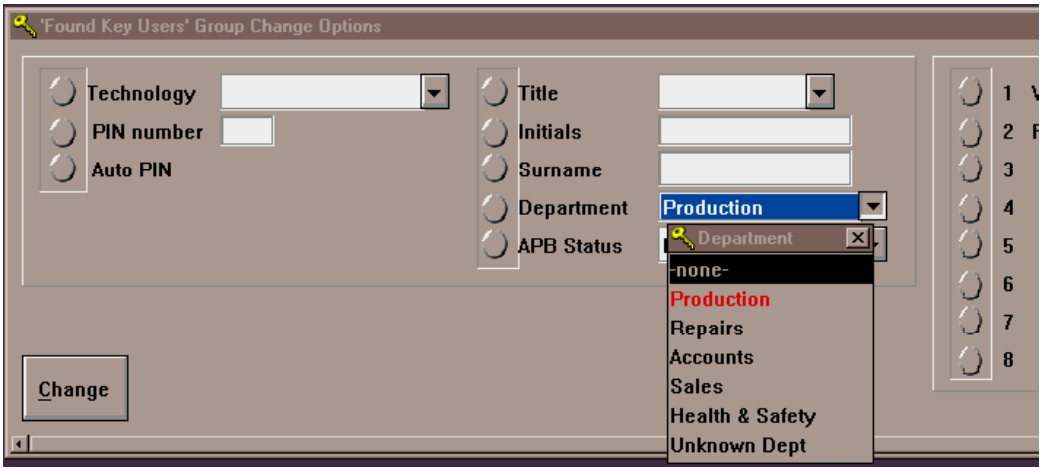


Fig 10.5 Group change window

Chapter Ten

MONITOR Option

Selecting this option displays the main log monitor which records any, or all, major system events. These events are:

- Internal system messages.
- MUX messages.
- Key transactions.
- Reader transactions.
- Print output.
- Search Output (including Muster Dumps).
- Time and Attendance Output.
- History Recall output.

This is the preferred option to display whenever the system is running without direct operator interaction. All major transactions can be seen at a glance and any necessary action taken through the use of the other options.

This monitor also has a Start Monitor on Message option (configured in ‘Monitors & Outputs’ in the CONFIG menu), which automatically opens the monitor window whenever one of the above configured events occurs.

Chapter Eleven

LOGIN Menu

If an operator is logged-out, this option opens the ‘LOGIN’ window to allow him/her to log in. All actions carried out from the ‘LOGIN’/’LOGOUT’ button are logged to all configured output devices and/or history files. If the operator is already logged-in, the following options are displayed:

Change Password

Allows the operator to change his/her current password. The old password must be entered first to ensure a valid operator is carrying out the operation, and the new password must be entered twice to verify correct entry.

Re-login

Logs the operator out and opens the LOGIN window.

Logout

Logs the operator out.

Chapter Twelve

CONTROL Menu

Plans and Maps

Allows the selection of a plan or map to be viewed. Also automatically opens the Zoom window.

Zoom Control

This opens the zoom control window (opened automatically when selecting the above). To alter the zoom ratio simply click on one of the pair of arrows on the required side of the ratio. Left-arrow decreases the number, right-arrow increases it.

A button is also supplied to reset the zoom ratio to 1:1.

MROC all loops

Manual Reader Over-Ride Command. Allows the selection of a pre-defined reader control function to be sent to all reader loops (effectively, to all readers).

For example, if it is necessary to evacuate the building rapidly, then all door latches could be opened by a manual over-ride command. The commands available are:

- Open Door.
- Reset Reader.

MROC a loop

Allows manual over-ride command of a single loop, with the same command options as ‘MROC all loops’.

MROC an Area

Allows a manual over-ride command to be sent to all readers within a previously defined Area. All defined areas have a text label. Same command options as ‘MROC all loops’.

MROC a reader

Allows a manual over-ride command to be sent to a particular reader. Same command options as ‘MROC all loops’.

Area Info

This operation opens a window which shows information on a selected Area. Selecting the ‘Area Info’ option from the Control menu opens a menu which lists all building Areas by name. Clicking on one of the areas then opens another window which contains information about the readers in that Area. This window displays the following information:

- The number of readers in the Area.
- The APB level of the Area.
- The maximum capacity limit of the Area.
- The current capacity of the Area.
- There is also a button labelled ‘Open MROC for Area’. This opens an MROC window, with the MROC commands as above, for that Area only.

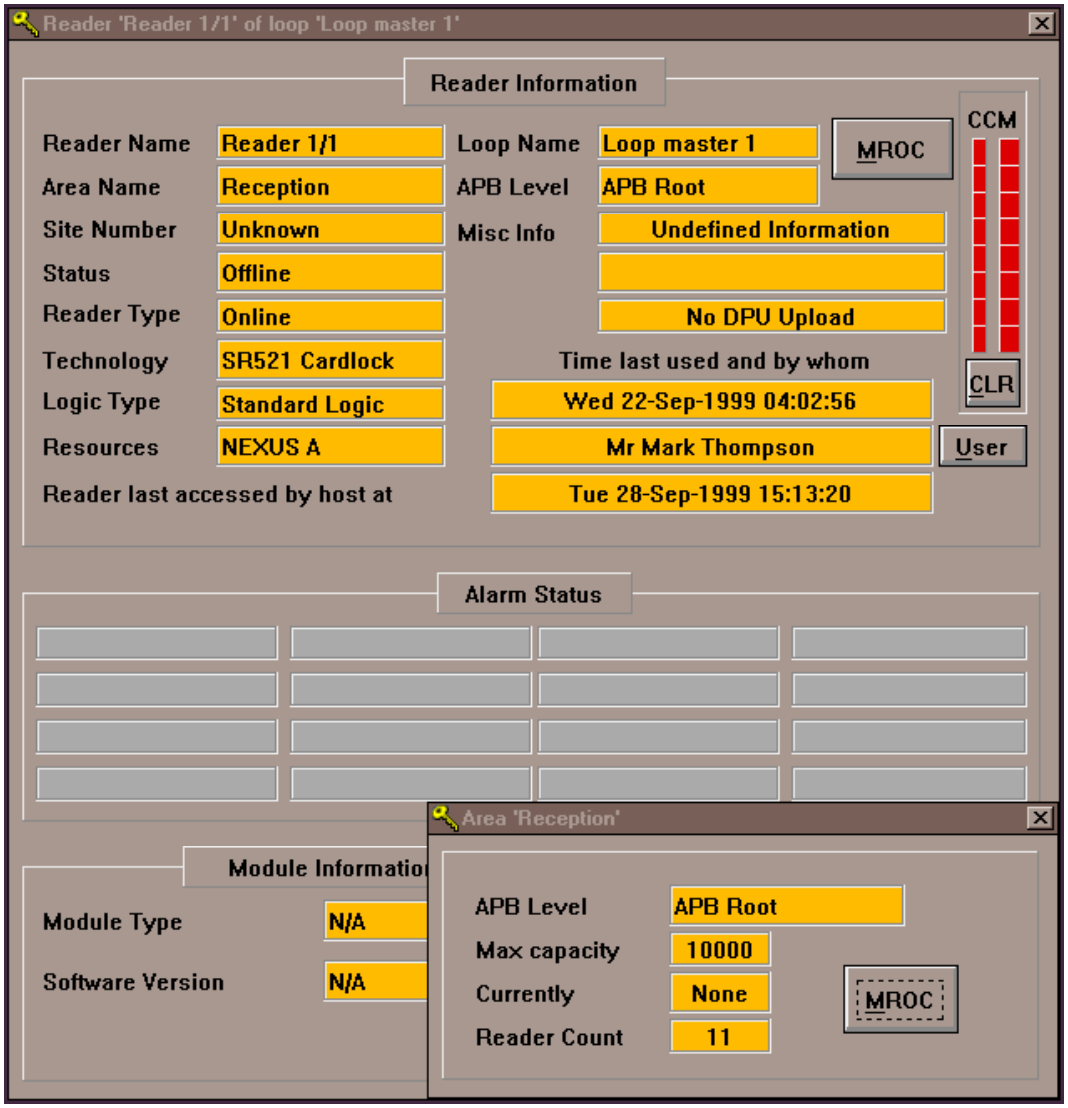


Fig. 13.1 Area and Reader Information windows.

Reader Info

This operation opens a window which shows information on a selected Reader. Selecting the ‘Reader Info’ option from the Control menu opens a menu which lists all Readers by name.

control menu

Clicking on one of the Readers then opens another window which contains information about the Reader. This window displays the following information:

- The Reader's name.
- Loop on which the Reader is placed.
- The Area in which the Reader resides.
- The COMM's loop the Reader's controlling MUX is connected.
- The current real time status of the Reader (i.e. On-line, Off-line, Pending).
- The Reader type (i.e. On-line, APB IN etc.).
- The Logic Type - the reader's reader script.
- The Reader's Technology (i.e. Watermark, Wiegand etc.).
- The Reader's Resources.
- The Reader's APB level, as defined by the Area.
- The Reader's current CCM state (where applicable).
- The last user to use the Reader and at what time.
- Real time indication of alarms from the Reader.
- The hardware type of the Reader (R100, R500, ISC etc.), version number and issue date of the software and the serial number.
- There is also a button labelled 'MROC'. This opens an MROC window, with the MROC commands as above, for that Reader only.

Reset MUXs

This operation sends a reset command to all multiplexors. This forces the multiplexors to request re-initialisation. The MUXs also reset all readers. This allows an operator to put the system into a defined and stabilised state.

Chapter Thirteen

History Recall

The History Recall System allows the operator to selectively search and display past historical events from the VISIKEY's past. Just about every single event is logged and has one or more properties for which a search can recognise.

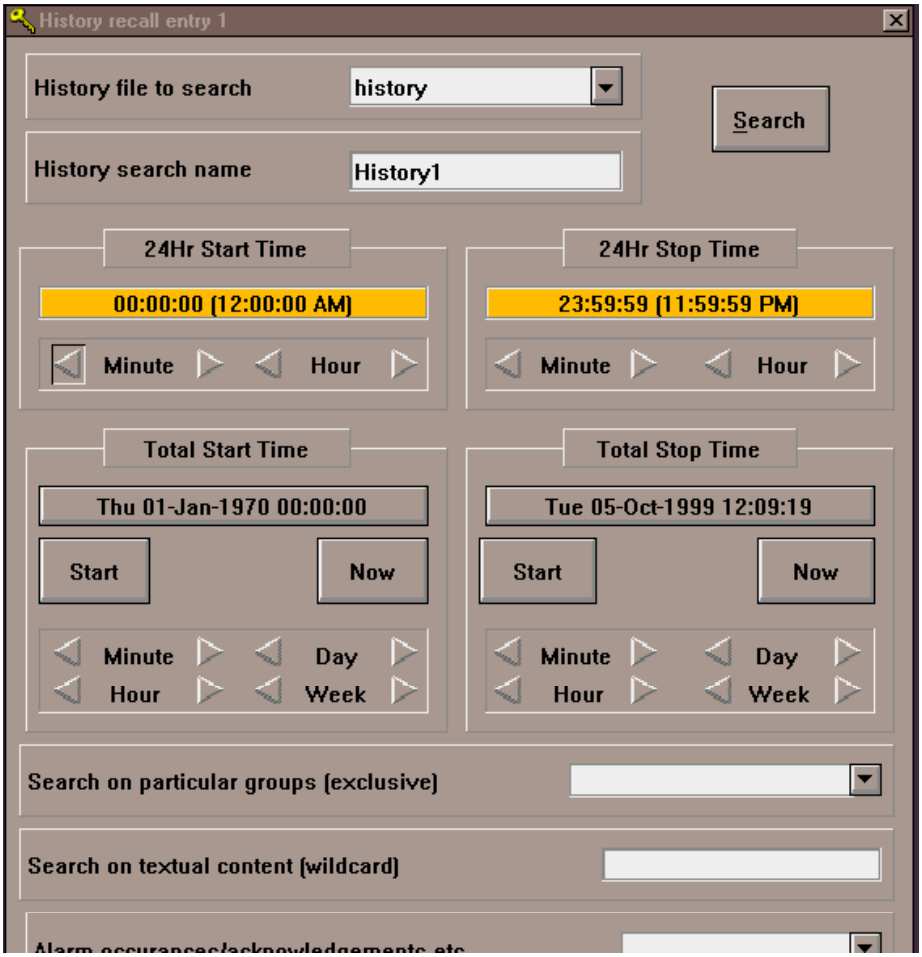


Fig. 14.1 The History Recall window.

The search system is a simple logical AND scenario, whereby each option specified must match if a record is to be displayed. The options are detailed below to aid comprehension:

History File to Search

This informs the VISIKEY which history file is to be searched, as the VISIKEY may have up to 7 different history files running concurrently, collecting the same or different information.

history recall

Start and Stop times

This informs the VISIKEY the time range in which records are to be checked. The earliest time cannot be before the creation of the history file specified, and the stop time cannot be beyond the current time. The times may be changed in steps of minutes, hours, days and weeks, and may be set to the earliest or latest time.

Search on Particular Group

This informs the VISIKEY which type of group should be sought. These groups are Internal, Multiplexor, Key Transactions, Reader Alarms, Print Output, User Searches, Time & Attendance Collation and other previous HRP output. These groups are used in the 'MONITORS AND OUTPUTS' section, to specify which messages are sent to which files, printers etc.

Search on Textual Content (Wild card)

In this, a textual string needs to be specified, and checks if any record contains this string.

Alarm Occurrences and Acknowledgements

This searches for all occurrences of the specified Alarm, including the actual alarm, it's acknowledgement, flushing, or being dropped from the bottom of the alarm stack.

Departmental Search

This searches for all occurrences of the specified user Department, including card transactions, user creation etc.

Search When a Certain Operation is Present

This searches for all occurrences of the specified Operator. This covers EVERY record when an operator is logged in. This is very useful to see what happened when 'ABC' was logged in last Thursday week; for example.

Reader

This searches for all occurrences of the specified Reader, including card transactions and reader alarms.

Area

This searches for all occurrences of the specified Area, including card transactions and all reader information from within that Area.

Keynumber

This searches for all occurrences of the specified Keynumber, including user creation and Key usage.

Technology

This searches for all occurrences of the specified Technology type.

history recall

Transaction

This searches for all occurrences of the specified transaction. These transactions include Permit Entry, Key Not Known Error, Time Zone Error, APB Error, Area Full, Area Access Error, and PIN error. This is useful for finding all illegal PIN usages within a week at a particular reader; for example.

When this window is initially opened, all options are cleared. The first operation to carryout is to specify which history file is to be used. As all other options are cleared, clicking on the search button now will retrieve everything from the file.

When a history file is almost full, warning will be given, and when it is full a further warning is given and it starts to overwrite the earliest entries. It is wise to print out the entire file when it first warns the user of being almost full. This can be carried out as explained in the previous paragraph. The printed copy may then be stored away for future referenc

Chapter Fourteen

System Configuration in Detail

The tasks which we will consider here are:

- Defining Day Types.
- Defining Week Types.
- Defining Year Types.
- Defining Areas.
- Defining Departments and their Access Rights.
- Defining User Fields.
- Entering a New Keycard Holder.
- Use of the Holiday Information Windows.
- Use of the Monitor Screen.

Defining Day Types

Day Types are defined on the Day Types window. To open this click on the ‘CONFIG’ option. A menu will appear. Click on the ‘DAY TYPES’ option then click on the 'New entry' option. A window will open. It will be entitled ‘TIME OF DAY ALLOCATION’. This is the window within which day types are defined.

Each defined Day Type receives a textual label i.e. a name, and is then addressed by this name whenever its use is required. To set your own day type click in the empty box next to the label 'Day name'. Then enter the day you wish to set i.e. Its label for example (See fig 16.1). The 'Day name' has been labelled '08 hour access' press the return key after the entry so that the data is recognised.

Each day type can have up to eight independently definable time zones within it (Slots 1 to 8). As you will see, most days will not require all of these but they allow for special customisation when necessary.

Look at the day (24 hour access). It has been set to allow entry from exactly midnight to 23:59pm. To enter this data, click on the dark grey box in the first time slot. Another small window will open. See fig. 16.2. This is the window that allows time entry. Click on the hour box of the start time. A drop down menu of hours appears (in 24-hour clock). Select one by clicking on it. It is automatically entered in the correct box. Now click on the minute box. Another menu appears. Select the number you wish and click. Once more it is entered automatically. Do the same for the End time boxes.

The times entered have automatically appeared in the slot 1 label. Now, simply close the small window by clicking on the ‘close’ icon and the data is entered into the appropriate column.

There are eight time entry slots and so eight time zones can be set for each day type. The times, which are set, do not have to be in any particular order.

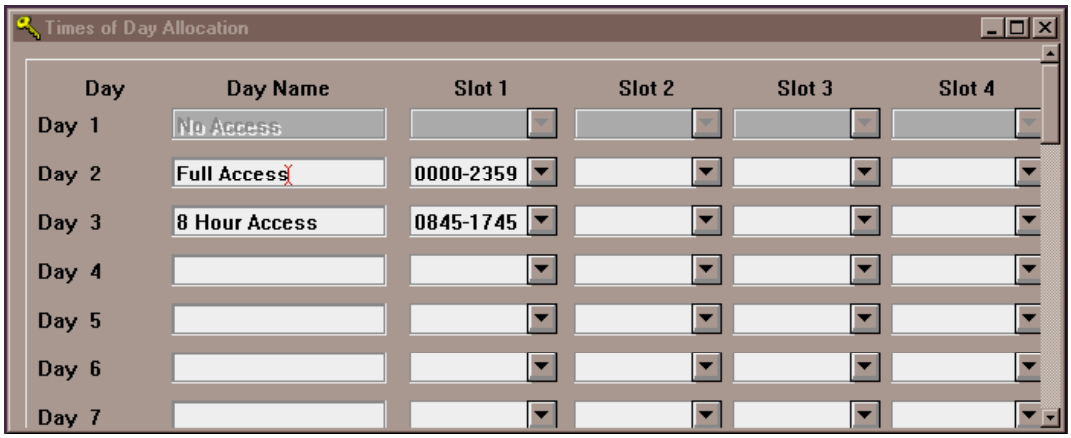


Fig. 16.1 Time of Day Allocation window.

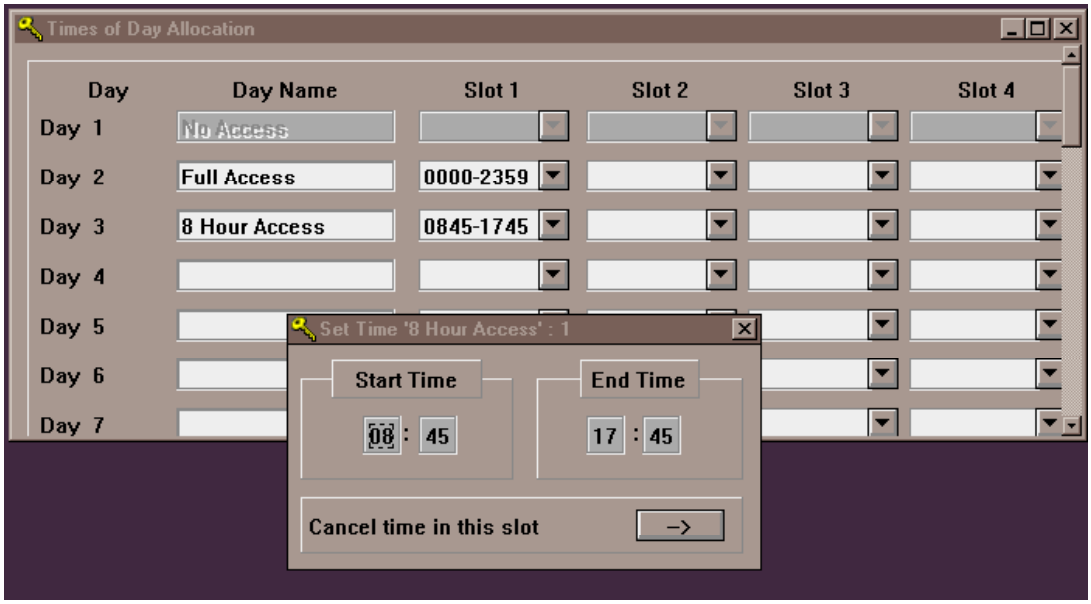


Fig. 16.2 Setting a Time Slot.

Continue to set up as many day types as you will need. There can be up to thirty-two. It is best to plan these out before you enter them. See the Chapter 15, ‘Planning Your System’.

Defining Week Types

Week Types are like Day Types, but instead of being defined in terms of times they are defined in terms of the Day Types previously mentioned. The Week Type window is opened through the ‘Config’ option menu and is entitled ‘Days of Week Time Allocation’ (See fig. 16.3.).

Each Week Type is addressed by a label i.e. its name and each label has seven columns, one for each day of the week. Into these columns are entered the Day Types that you wish each day in that particular Week Type to be.

To enter the name of a Week Type simply click on the new entry option in the week type menu, then click onto the empty box next to the 'Week name' label. The cursor will appear. Now type in the name you wish to give that particular Week Type and press the Return key. The Week Type name has now been entered. Now enter a Day Type for each day of the week. An entry for every day is already set. This is the ‘No Access’ Day Type. You can either leave this as set or change it to suit your own requirements. To change the entry, click on the relevant box and a menu will appear listing all of the day types you have previously defined. Select one of these with the pointer and click. It is entered into the box for that day (See fig. 16.5 & 16.6). You can change these entries as often as you wish.

Once you have set your first week type you can set others simply by repeating the procedure. The VISIKEY software will allow you to configure up to thirty-two different Week Types.

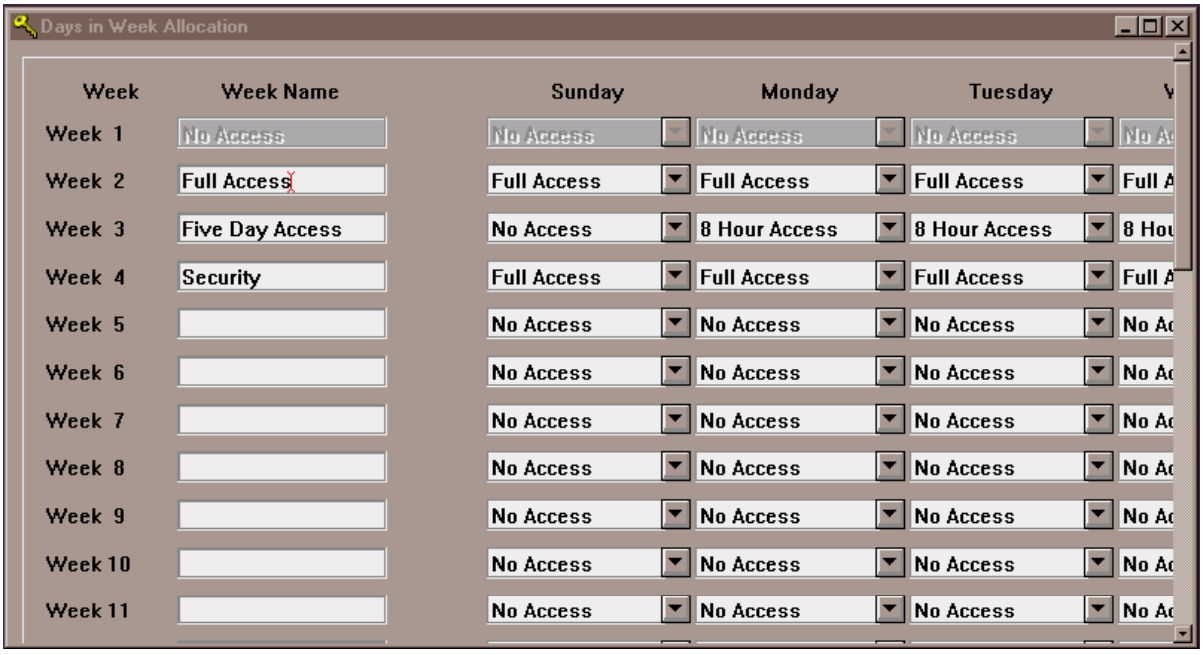


Fig. 16.3 Days of Week Allocation.

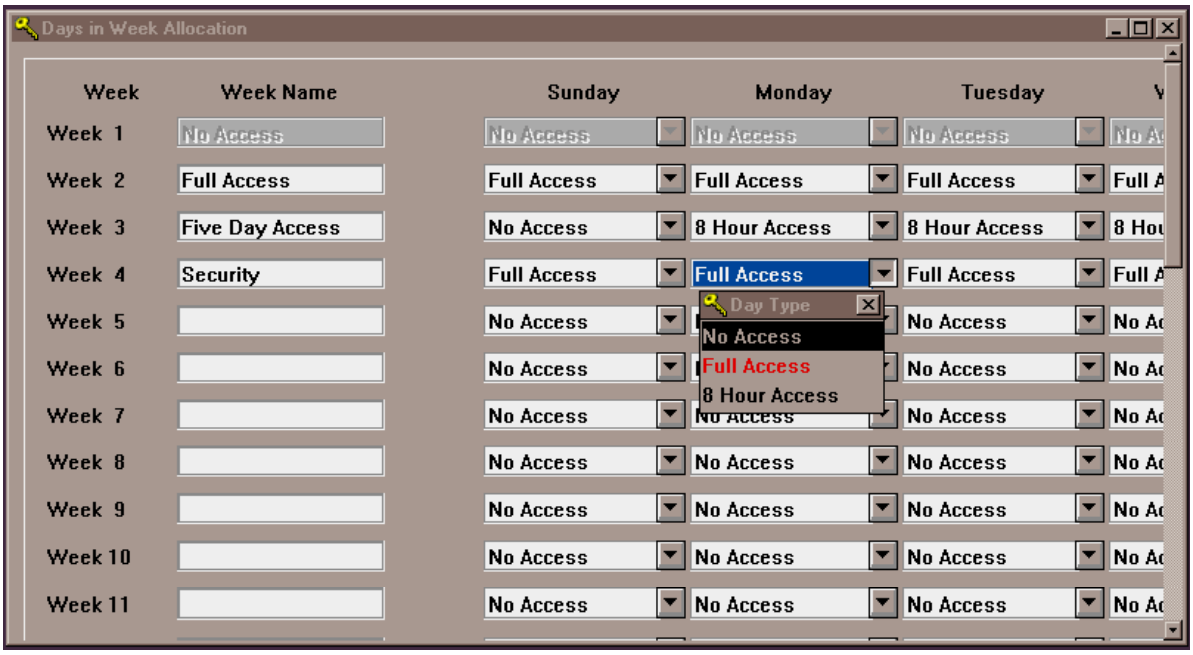


Fig. 16.4 Change a Day Type within a week.

Defining Year Types

Year Types, like Week Types, are made up of smaller items. Each Year Type is built up from 53-Week types, each week being individually assignable. To build up a year with the same week, simply set the first week to the required Week Type, and then click on the replication button to the right of the week. Select the number one. This means every week of the year will be set to the same as the first.

The replication system allows the quick and simple setting of shift patterns. If replication 2 is selected, then every other week is set, and if replication 3 is selected, then it would be every 3 weeks. Note that only the weeks subsequent to the one being selected will be modified by replication.

There are 32 different Year Types, but the first Year Type is permanently set to ‘No Access’. The Years Types may be changed as frequently as required, with the modification being immediately brought into force.

Defining Areas

An Area is a logical area in which Readers reside. An Area may have any number of entry and exit Readers, with or without APB protection. If APB protection is enabled, then an additional option of Capacity is possible, to set the maximum number of Keycard Holders in the Area.

To create an Area, click on the Area name box and enter a name for the given Area. If Anti Pass Back (APB) is required, set the Area's depth into the building (APB Level). To calculate this number, assume the outside world is zero, then the foyer is 1, and so on - working in recursive circles.

To limit the number of Keycard Holders in an Area, set the capacity option to the maximum required. When an Area is full, no one else is allowed in until someone leaves the Area.

Defining Departments and Their Access Rights

Whenever a new Keycard Holder is defined, as described earlier, he or she must be assigned a department, and it is through this departmental assignment that a Keycard Holders actual access rights within the building are set. All Keycard Holders in a department have the same access rights and these are defined through the 'Departments' window.

To select the 'Departments' window, simply select the 'Departments' option from the 'Config' menu. The Departments window will appear. In fig. 16.7 the names of some Departments have already been entered and one is in the process of being entered.

To enter a Department name, click on the 'New entry' option. Clicking on this opens a second window entitled 'Access Rights' and it is within this second window that the access rights of the particular department are defined. These access rights are defined in terms of Areas and Year Types. Type in the name of the Department and press the Return key.

You will notice that every Department name has a thin, grey button to the right of it to open the access rights window.

The Access Rights window is shown in figs. 16.8, 16.9 and 16.10.

If you do not enter a particular Area into the Access Rights window for a particular Department, that Department will, by default, have no access to that particular Area.

Once all of the Areas have been entered into the Access Rights window for a particular Department you can then enter the access Week Type for that Area. Look at figs. 16.8 to 16.10. While the Sales Department can enter the main office, and the demo room, they have no access to the stores. The access rights of the sales department are changed to give normal access to stores.

When planning the Year types to enter into the Access Rights menu, it is often better to work backwards. Decide which Areas a Department should NOT have access to and then you can ignore these entries, as they are blank by default.

Now, consider those Areas to which a Department must have access. Decide on the times at which a Department should have access to a particular Area and which Year type this is. If it is not one of your previously defined Year types than you can return to the Year types menu and define it. Most organisations will find that most of their employees can be catered for using a small core of Year types, leaving the others free for more specialised access requirements.

Having decided on which Year type satisfies the access requirements for a particular Area and Department, this can then be entered alongside the Area name in the corresponding Access Rights window. Simply click on the dark grey box opposite the required Area. A menu will drop down. Select the required Year type and click. It is automatically entered. Continue this procedure for every Area for each Department in turn. Once this is done, the Access Rights for all Keycard Holders have been defined.

Fig. 16.7 Department List.

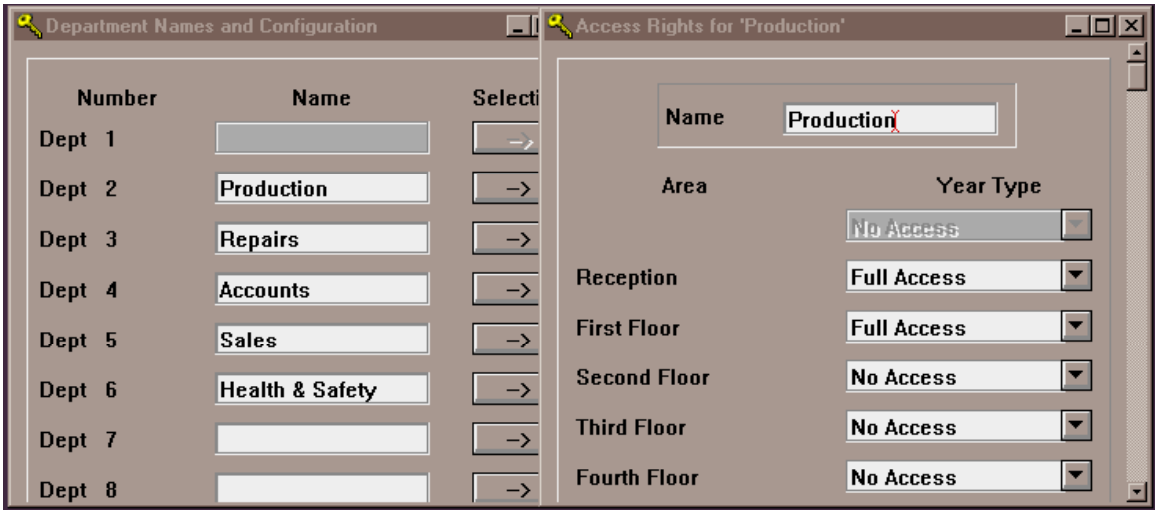


Fig. 16.8 Department List with Access Rights for ‘Sales’.

Defining User Fields

The VISIKEY has two separate types of user configurable fields, those which contain the answers to yes/no questions e.g. is the Keycard Holder a first-aider; and those which hold a longer piece of textual information e.g. a date of birth.

Textual User Fields are provided in the VISIKEY to allow for the customisation of Keycard Holder records. A textual User Field consists of three parts;

1. The text of the field which is its title e.g. ‘first-aider’ or ‘D.O.B.’
2. The default information contained in the field.
3. The size of the field.

To open the User Fields window, select it through the Config. Menu. See fig. 16.11. Both types of field can be customised through this window. To set a yes/no field (which is controlled through the grey toggle buttons), click on one of the eight grey boxes in the ‘Marker’ section. When the cursor appears, type in the text. This text will now appear in the Create User menu when it is next opened and you can set a yes or no answer to it for every user. As an example, this field could have the option ‘Fire-fighter’ added.

The second type of field is slightly more complex. There are five sub-fields and each has a text message and can contain up to 16 characters or numbers about a user in answer to that message. As an example, this field has been pre-set with ‘Sex’ and ‘D.O.B.’ in the figures, but all five separate areas of the field can be changed as desired.

To set the message for a sub-field, click on a box below the ‘Sex’ and ‘D.O.B.’ messages already set and enter the message text when the cursor appears. Now click on the box across from this (beneath the ‘m’ and the ‘dd-mm-yyyy’). This box will appear ready to accept

information when the Create User window is next selected. In this box you are setting the default contents for that field.

Look at the entry for the D.O.B. option. It gives the specified format in which you are supposed to enter the information about a person's birth. It is to consist of two numbers for the day (always two and no fewer - so the third would be entered '03'), a dash, then two numbers for the month (e.g. July would be '07') and four numbers for the year e.g. 1967. This in this case would look like *03-07-1993*.

The system will not distinguish between letters and numbers, or any other characters, in these entries as these fields are totally configurable and the VISIKEY software does not filter them in any way. You should, therefore, make the format in which you expect data entry, as clear as possible. If you wished to enter data for 'Car Registration' you would set the default contents to seven characters, such as seven 'x' dummy letters. You can use any letters you wish here to indicate the information format.

Once you have entered the text and answer format for your field, you must then tell the VISIKEY how much data to expect. The number of bytes of information is the same as the number of characters in the answer box.

Firstly, click on the left-hand dark grey box between the text and answer columns. This tells the VISIKEY software where your data will start. A menu will drop down. Click on the number that is one greater than the number in the right-hand dark grey box on the level above. This number will now appear in the lower left-hand box. Now click on the right-hand dark grey box on the same level as the left-hand box. Again a menu drops down. Add the number of characters in the answer you expect to the number in the left-hand box. Click on this number. This tells the VISIKEY software where the data for that sub-field ends.

Although this procedure might sound quite complex, it is in fact very simple and easy to become accustomed to. User definable fields can be very useful and the questions asked through them should be carefully considered.

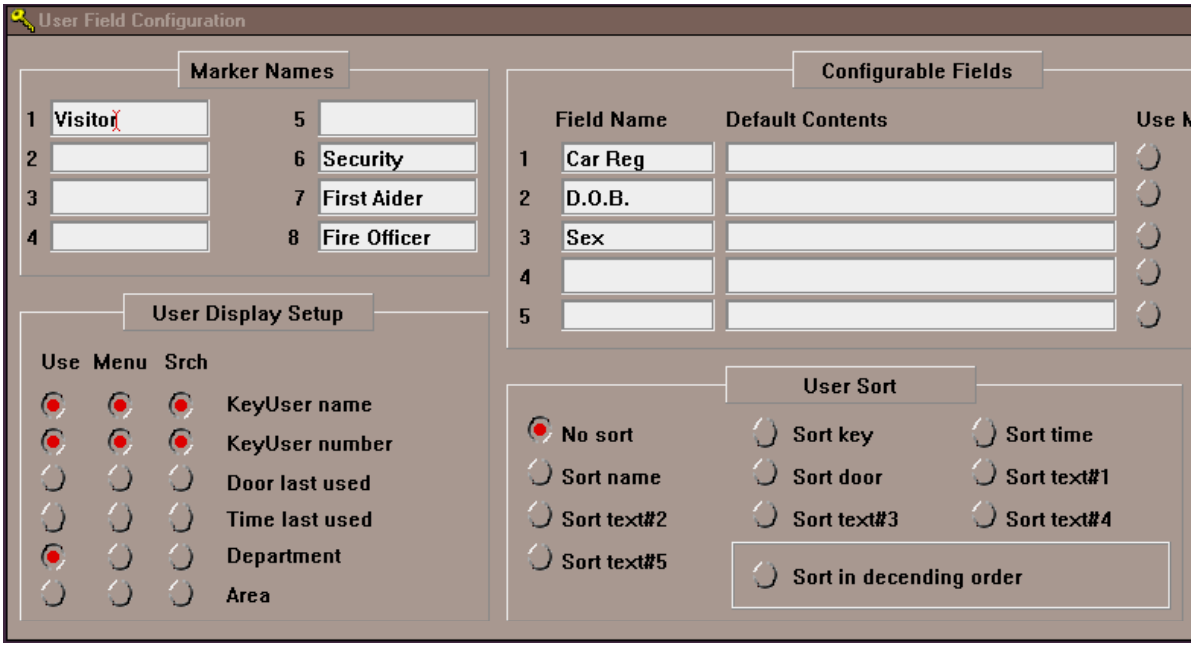


Fig. 16.11 User Field Configuration window.

Entering a New Card Holder

The VISIKEY can support up to 65 thousand Keycard Holders, each of which can have certain departmental limits of building access. The window used to enter the details of a new Keycard Holder is shown in fig. 16.11. This window can also be used to edit previously entered details.

To open this window, first select the ‘Key user base’ option from the 'Primary option menu' by clicking on it once. A menu will pop up. Move up to the ‘Create new user’ option and click. The window, as in fig. 16.12 will now appear.

Once the window is opened look at the categories to be entered. Now look at fig. 16.12. Some of these categories have already been filled-in by default. These can be changed if required. Information is entered into the new Keycard Holder screen in the following ways:

Textual Information

By placing the cursor in a box and typing in the information directly. The name, key number and PIN are entered in this way, ‘Sex’, ‘date of birth’ (D.O.B.) plus other information for other operator definable fields are also entered in this way. To place the cursor in a box, move the pointing arrow over the box to the place you want the cursor to be and then simply click. The cursor will appear in the box. If the cursor is not where you want it in the box, move it either by re-pointing the arrow and clicking again, or by using the arrow keys on the keyboard.

If you place the cursor in the wrong box, simply move to the correct box and click and the cursor will appear there automatically.

Boxes that require information to be entered in this fashion are coloured light grey.

Note that using a ‘Local’ reader with a Keycard will insert a key number into the key number field automatically, removing the necessity to type in the number manually.

Yes/No Information

By Yes/No toggling of ‘buttons’, such as those first seen on the password menu. The User Markers column operates this way. Click on the buttons to toggle them on or off.

Toggling one of these buttons to ‘on’ places the user in that particular category. Up to eight categories can be defined and these can be used as search criteria when it is necessary to find certain users e.g. first-aiders.

The lines;

‘Key User record marked for deletion on next packing’

And;

‘Prevent user from using key’

Also operate by toggle buttons. Do not, of course, set the deletion toggle to ‘on’ unless you want to delete the user from the user base!

Drop Menu’ Information

Dark grey boxes should be clicked on to enter information. Once clicked on, a menu will appear of all the information that is allowed to go into that box. Simply move the arrow down the menu until it points at the data you wish to enter and then click. The data is automatically entered for you.

The ‘Title’, ‘Department’, and ‘Technology’ boxes work this way.

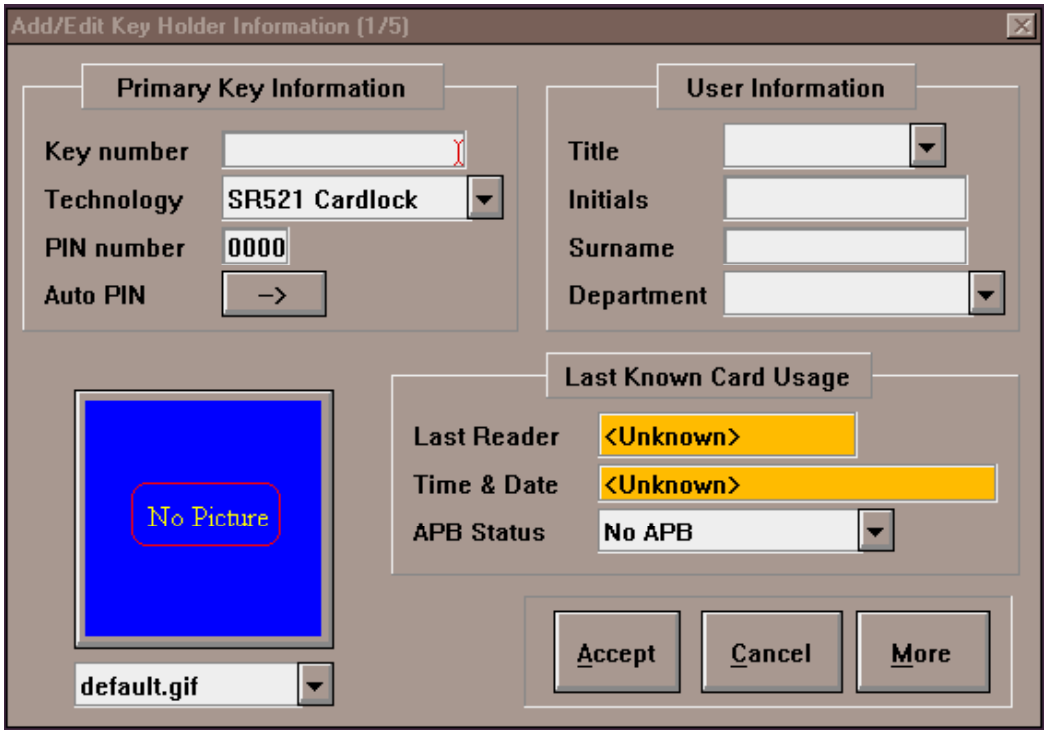
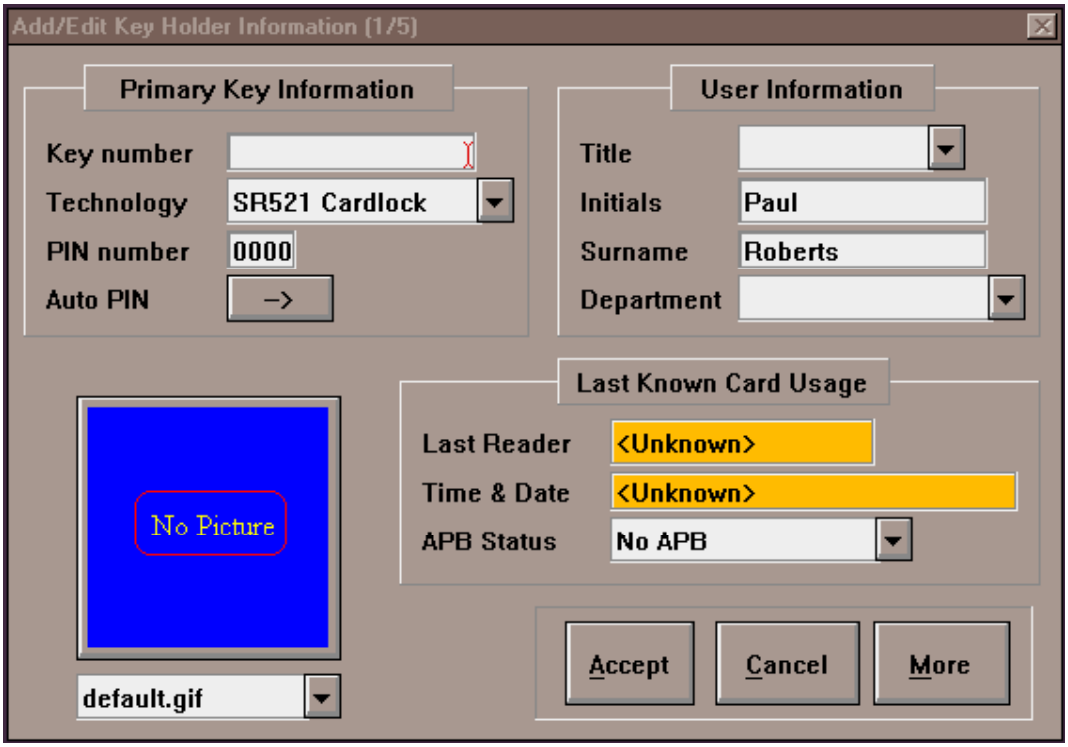


Fig. 16.12 Blank User Record.



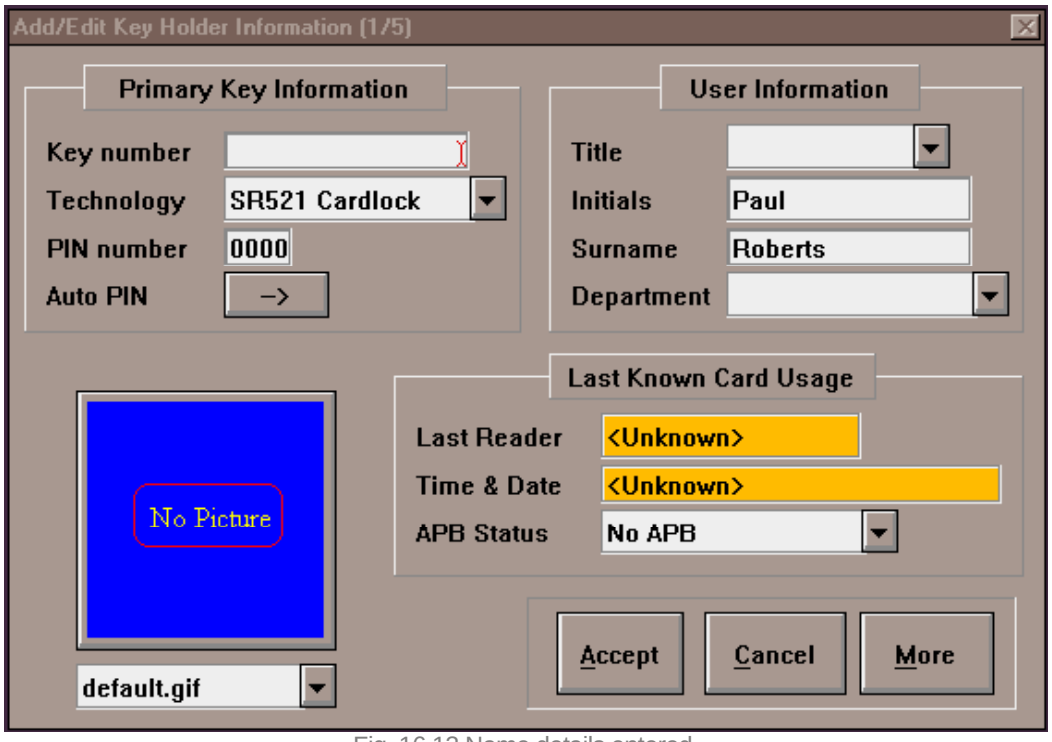


Fig. 16.13 Name details entered.

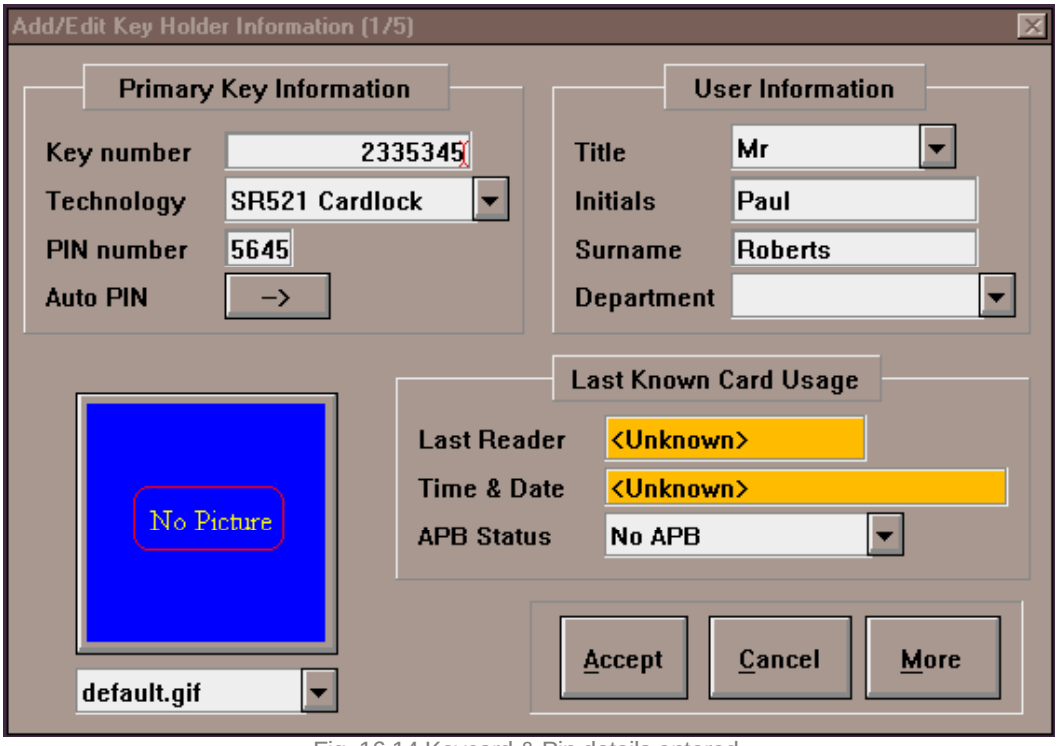


Fig. 16.14 Keycard & Pin details entered.

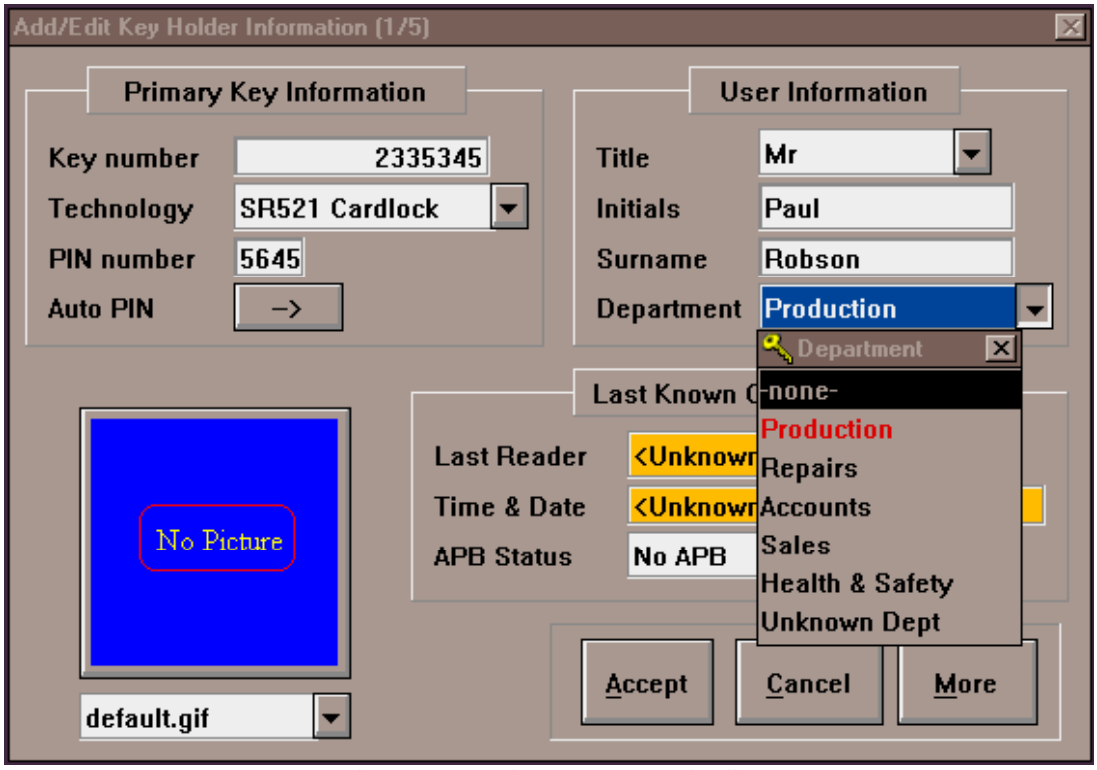


Fig. 16.15 Entering Department details.

Button Click Information

The Auto-PIN (provided you have set it - see Section 10.8) and 'Automatically prevent Key usage at' boxes are controlled by clicking on the raised buttons and small raised arrows to enter data.

Now let us consider how the data was entered in fig. 16.13 and 16.14. Firstly, the name of the key user was entered by clicking on the relevant boxes and then typing in the information before pressing the Return key at the end of each box i.e. both after the initials and after the surname. The key number and PIN number is also entered in this manner.

The 'Title' and 'Technology' data were entered using menus, as in method two. In fig. 16.15, this method is being used to enter data into the 'Department' box. Once the Department has been entered, you should then set the APB level. Finally, enter the data into the definable fields, the key user could be tagged as a first-aider, for example, by clicking on the relevant toggle button.

The definable fields of 'sex 'and 'date-of-birth' are also entered using method 1.

Three more categories of user definable textual information are available and these are also entered by method 1.

When setting the time at which to automatically prevent key usage, there are three options - ‘now’, ‘never’ (which displays the word ‘Indefinite’) and a specific time and date. Click on either of the two large buttons in the bottom right-hand corner to select ‘Now’ or ‘Never’. To select a specific time and date, select ‘Now’. The current time and date will be displayed and you can alter these settings by clicking on the arrows in the small panel at the bottom left. A single click on each arrow will alter the relevant piece of data in plus or minus one steps. When you have the time and date you want, simply stop. You cannot go back past the current time and date.

Once the configured time and date have been reached, the ‘Prevent Card Usage’ button is automatically set - rendering the card useless. The configured output devices are informed of the event.

When you have entered the data in the key user window to your satisfaction, simply click on the ‘Update’ box. Remember that you can alter data as much as you wish, going back to boxes and changing them until you are completely satisfied. It is only when you click on ‘Update’ that the record will be entered into the system. If you decide not to enter the user into the system, simply click on abandon and the data will be ignored and the window will close.

The entering of new key users is registered on the monitor screen and on whichever external devices are set to receive that category of monitor information.

Multiple Keycard Holders may be entered with the same details. All that is required is a surname (possible a dummy name), technology type, initial Key number and Department. Up to 500 entries may be created by setting the appropriate entry at the bottom of the User Record. The increment type, BCD or HEX means whether or not the resulting numbers can contain HEX digits (i.e. ‘A’ to ‘F’). This is generally set to BCD.

<u>NOTE</u> The technology label ‘Watermark’ indicates that the user has been assigned as a Keycard holder with a Watermark card. ‘Watermark’ is a brand name for a specific type of card with special properties, namely that once data is set on it cannot be altered or removed. The cards will come with information about the ten digit number set on them when they are purchased by the company and it is this number which must be entered as the Keycard Holders key-number when he is issued with the card. Key-numbers cannot be operator chosen, they must be as set on the cards.

See Appendix 3 for more information about Watermarked cards.

Use of the Holiday Information Windows

The Holiday windows are used to set override conditions on normally set access rights. These overrides can be set to occur on specific, operator-definable, dates i.e. ‘Holidays’.

To open the Holiday window, select the option from the Config. menu. The window will open and appear as in fig. 16.16 the current date is marked in grey.

To select the date for which you wish to overlay holiday information on normal access rights, simply click on it in the window. A new window will open entitled ‘Access Rights on’ and the

date selected. A list of departments is given on the left and their access rights on this date are displayed alongside. See fig. 16.17

If the access rights for a Department are left set at <Normal Access> (as automatically defined by the system) then that Department will have the same access rights as set through the normal Access Rights window.

To see the other options, click on the dark grey bar (set by default to <Normal Access>). Every previously defined Day Type is available. If you have previously defined a Day Type labelled 'Normal Access' yourself then there will be two of these available to choose from, but the VISIKEY will be able to distinguish between them. Move down the menu and click on the Day Type which you wish to enter.

Go through and set the access rights for that particular date for every department. If you do not set a new Day Type then the <Normal Access> option will remain. A 'No Access' Day Type, as automatically defined by the system, will be available. Use this to label those departments which are not allowed building access on that date.

Those departments which are allowed access on that date will have the same Area access rights as a normal day, but the times of this access may have changed, depending on whether a new Day Type has been specified.

Move through the year setting holiday access rights as necessary. When you are finished simply click on the close icon.

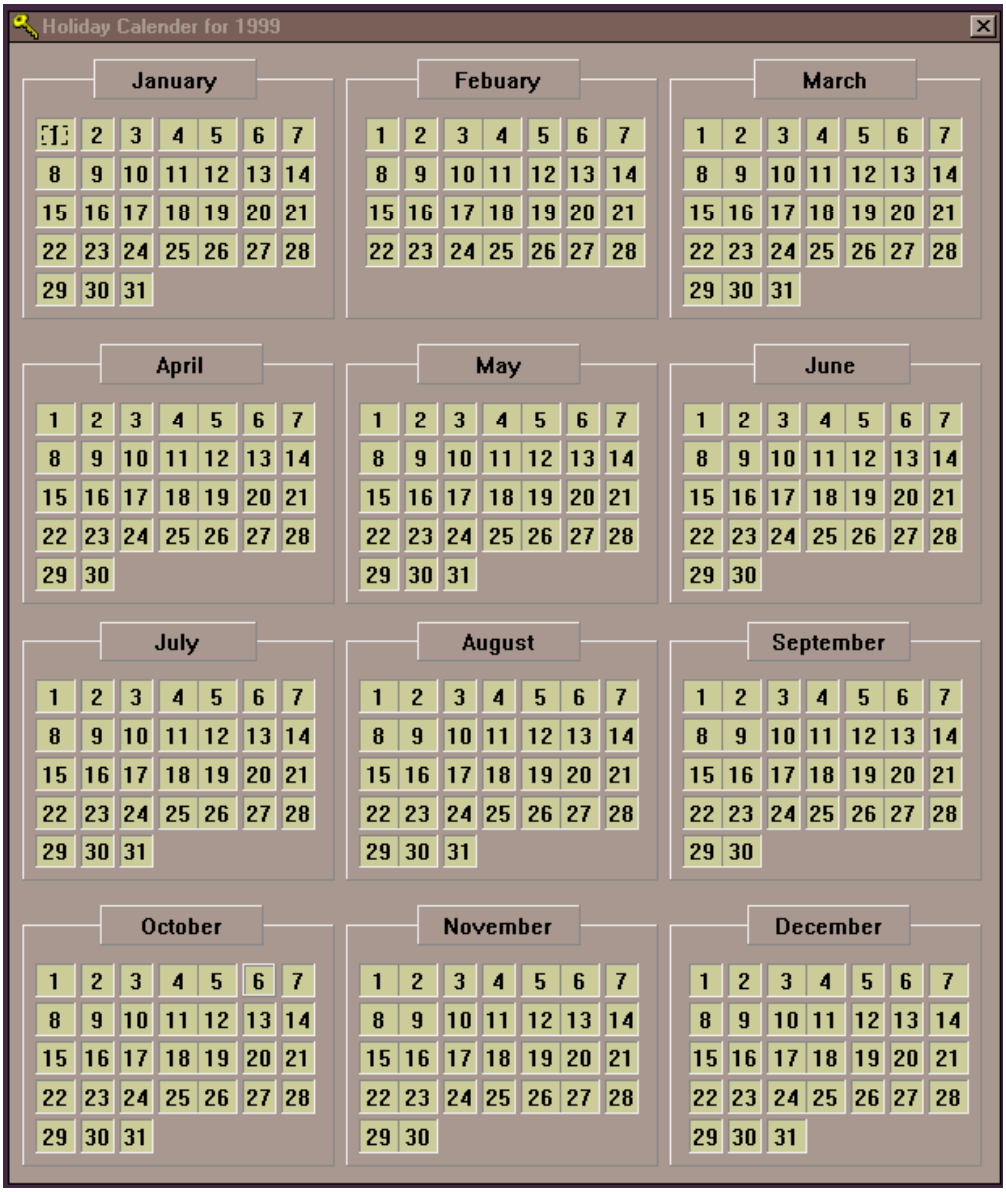


Fig. 16.16 The Holiday Calendar window.

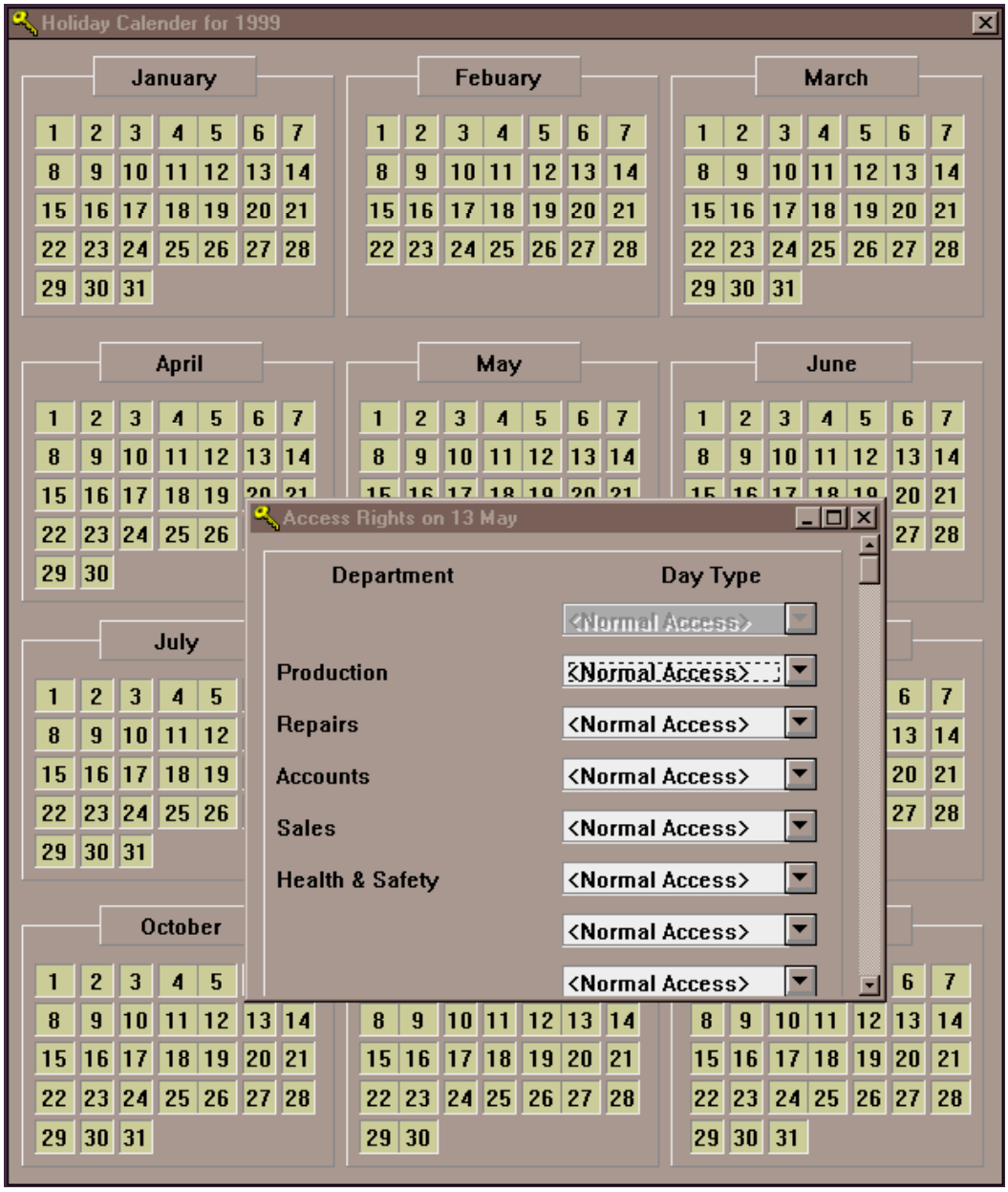


Fig. 16.17 Holiday Access Rights for July 3rd.

Use of the Monitor Window

The Monitor window is opened by clicking on the Monitor option. When first opened it fills the entire screen, but you may wish to re-size it (see fig. 16.17). On this screen are displayed the major transactions which occur within the system. These are:

- Internal System messages e.g. Login, addition of a user.
- MUX messages.
- Card Transactions.
- Reader Messages e.g. alarm messages.
- Print output.
- User Search results (including Muster Dumps).
- Time and Attendance output.
- History Recall output.

The Monitor window is best displayed permanently, but you may not wish it to cover the whole window. If you do re-size the window then move the side bar down so that you are looking at the bottom end of the window display as this is where all of the latest transactions are reported.

The Monitor window can be set to open automatically on any monitor output. Simply set the 'Start Monitor on Message' option with 'Monitors and Outputs' option with the CONFIG menu. The window will open with the same size and in the same position as it was when it was last closed.

Other monitors can also be set e.g. a printer which is set to monitor certain transactions. Their can be up to eight monitors including the monitor window. Each monitor can be set to record any combination of the monitored events as mentioned above.

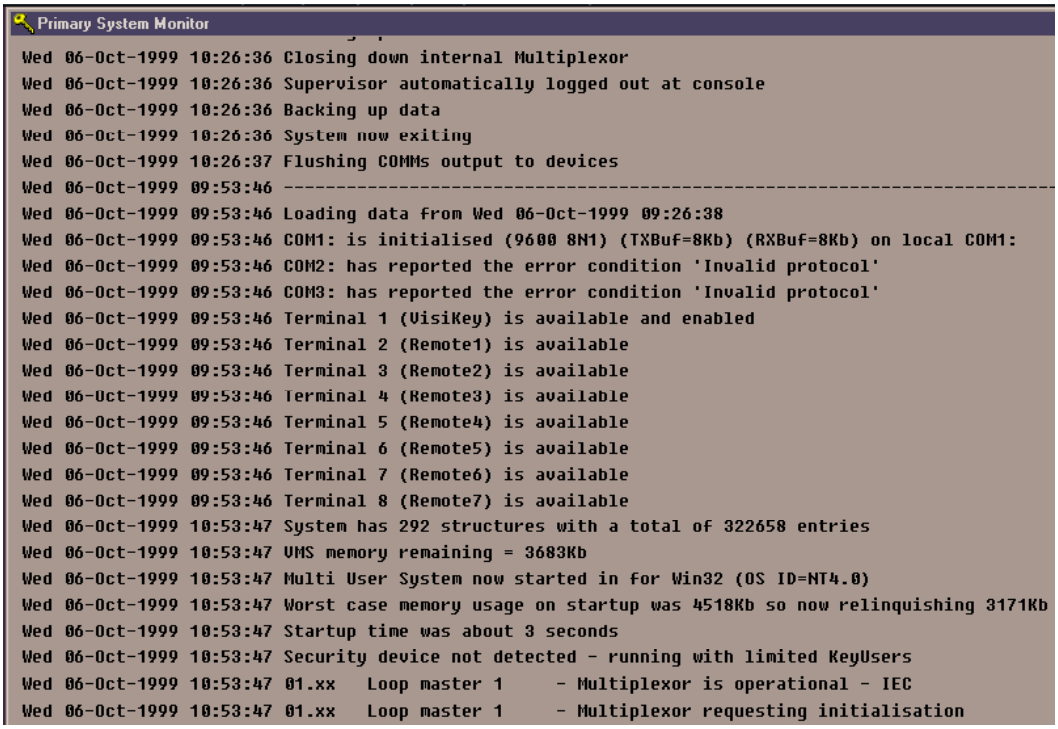

Primary System Monitor
Wed 06-Oct-1999 10:26:36 Closing down internal Multiplexor
Wed 06-Oct-1999 10:26:36 Supervisor automatically logged out at console
Wed 06-Oct-1999 10:26:36 Backing up data
Wed 06-Oct-1999 10:26:36 System now exiting
Wed 06-Oct-1999 10:26:37 Flushing COMMs output to devices
Wed 06-Oct-1999 09:53:46 ----------
Wed 06-Oct-1999 09:53:46 Loading data from Wed 06-Oct-1999 09:26:38
Wed 06-Oct-1999 09:53:46 COM1: is initialised (9600 8N1) (TXBuf=8Kb) (RXBuf=8Kb) on local COM1:
Wed 06-Oct-1999 09:53:46 COM2: has reported the error condition 'Invalid protocol'
Wed 06-Oct-1999 09:53:46 COM3: has reported the error condition 'Invalid protocol'
Wed 06-Oct-1999 09:53:46 Terminal 1 (VisiKey) is available and enabled
Wed 06-Oct-1999 09:53:46 Terminal 2 (Remote1) is available
Wed 06-Oct-1999 09:53:46 Terminal 3 (Remote2) is available
Wed 06-Oct-1999 09:53:46 Terminal 4 (Remote3) is available
Wed 06-Oct-1999 09:53:46 Terminal 5 (Remote4) is available
Wed 06-Oct-1999 09:53:46 Terminal 6 (Remote5) is available
Wed 06-Oct-1999 09:53:46 Terminal 7 (Remote6) is available
Wed 06-Oct-1999 09:53:46 Terminal 8 (Remote7) is available
Wed 06-Oct-1999 10:53:47 System has 292 structures with a total of 322658 entries
Wed 06-Oct-1999 10:53:47 VMS memory remaining = 3683Kb
Wed 06-Oct-1999 10:53:47 Multi User System now started in for Win32 (OS ID=NT4.0)
Wed 06-Oct-1999 10:53:47 Worst case memory usage on startup was 4518Kb so now relinquishing 3171Kb
Wed 06-Oct-1999 10:53:47 Startup time was about 3 seconds
Wed 06-Oct-1999 10:53:47 Security device not detected - running with limited KeyUsers
Wed 06-Oct-1999 10:53:47 01.xx Loop master 1 - Multiplexor is operational - IEC
Wed 06-Oct-1999 10:53:47 01.xx Loop master 1 - Multiplexor requesting initialisation

Fig. 16.18 Inbuilt Monitor window.

Chapter Fifteen

Planning Your System

Having read the previous section you should now be familiar with the capabilities of the VISIKEY. We will consider here how to plan a system whose details can then be entered as previously described.

The first requirement is a plan of the layout of your organisation. It does not have to be to scale but should include the locations of all readers and their APB numbers, and also notes of any special requirements. Remember, APB numbers increase as more restricted levels are reached. To calculate the APB level of a certain Area, simply count the number of APB registered readers through which it is necessary to pass to reach the current Area. Work from the outside in, the first APB Area being level 1. There can be up to 128 APB levels.

Now assign a number to all of the readers on the plan. These are the numbers which the VISIKEY will use to address them. Each reader must, obviously, have a completely unique number. This is set in hardware. Once the readers have been configured, each may be assigned a name through the VISIKEY software and can then be addressed by that, but for actual system installation and commissioning, each reader must be given a number.

Readers are arranged in loops, and all the readers in any one loop addressed with a single Manual Reader Override Command (see ‘MROC a Loop’). Any one loop can have up to 128 readers in it and there can be up to 18 loops. All readers can be addressed singly if necessary (see ‘MROC a Reader’). The grouping of readers into loops depends on which control box they are attached to and will not be considered here.

Chapter Sixteen

Programming a Reader

Readers in the VISIKEY can be individually programmed. It is not, however, necessary to write a separate program for every reader. Once written, each program can be applied to as many readers as required. Programming readers allows their responses to be configured precisely to the specific needs of any application.

Readers can be programmed through the VISIKEY computer. The method of programming combines Boolean Algebra, to allow logical operations, and Reverse Polish Notation (RPN). If you require further information on either of these topics, please consult Appendix 3.

Each reader can have one Boolean expression for each Output line, Alarm line and for each internal Timer. There are 16 of each of these, so a reader can be programmed with up to 48 separate expression.

Entering a Program

To enter a program you must first open the Reader Logic Library window by selecting the 'Reader Logic' option on the 'CONFIG' menu. Click on a Name bar and give your program a name. Now select the grey 'button' to the right of this name. This opens the Reader Logic window which allows you to enter your program. A line of program can be entered opposite each of the sixteen Output lines, Alarm lines and Timers, eight resetable latches and time zones, reader system alarms, and transaction verification. You do not have to program all of the lines. Leave blank any that you do not wish to use. The window moves sideways to accommodate all the lines as necessary. Press the Return key after each line that you enter. Once you have entered all of your lines, simply close the window. Open another window if you wish to enter another program, or return to the system options by closing the Reader Logic Library window.

Output lines 1 to 16 are actual, physical output lines which control relays inside the reader units. These relays can be connected to whatever external equipment is considered necessary. For example, one of the relays should be connected to the circuit which activates the door lock mechanism, thereby allowing the reader to operate the door. Other output line relays could be connected to, for example, an alarm bell or a siren. The setting of these relays is a hardware task, and should be considered when the VISIKEY is being installed.

The Alarm lines are read into the VISIKEY computer and are detected by the system software. This software can then configure the system response to the alarm condition. The VISIKEY software could trigger alarm messages as previously set, display 'Alarm Windows', make audible alarms, and/or create Muster lists on selected groups.

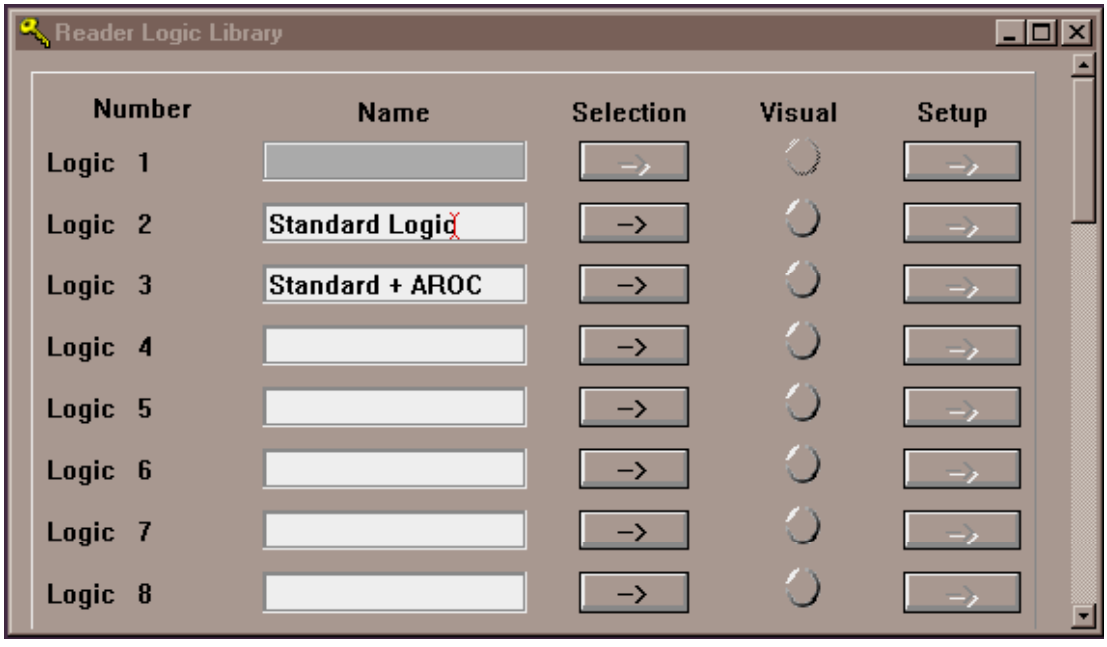


Fig. 18.1 The Reader Logic Library window.

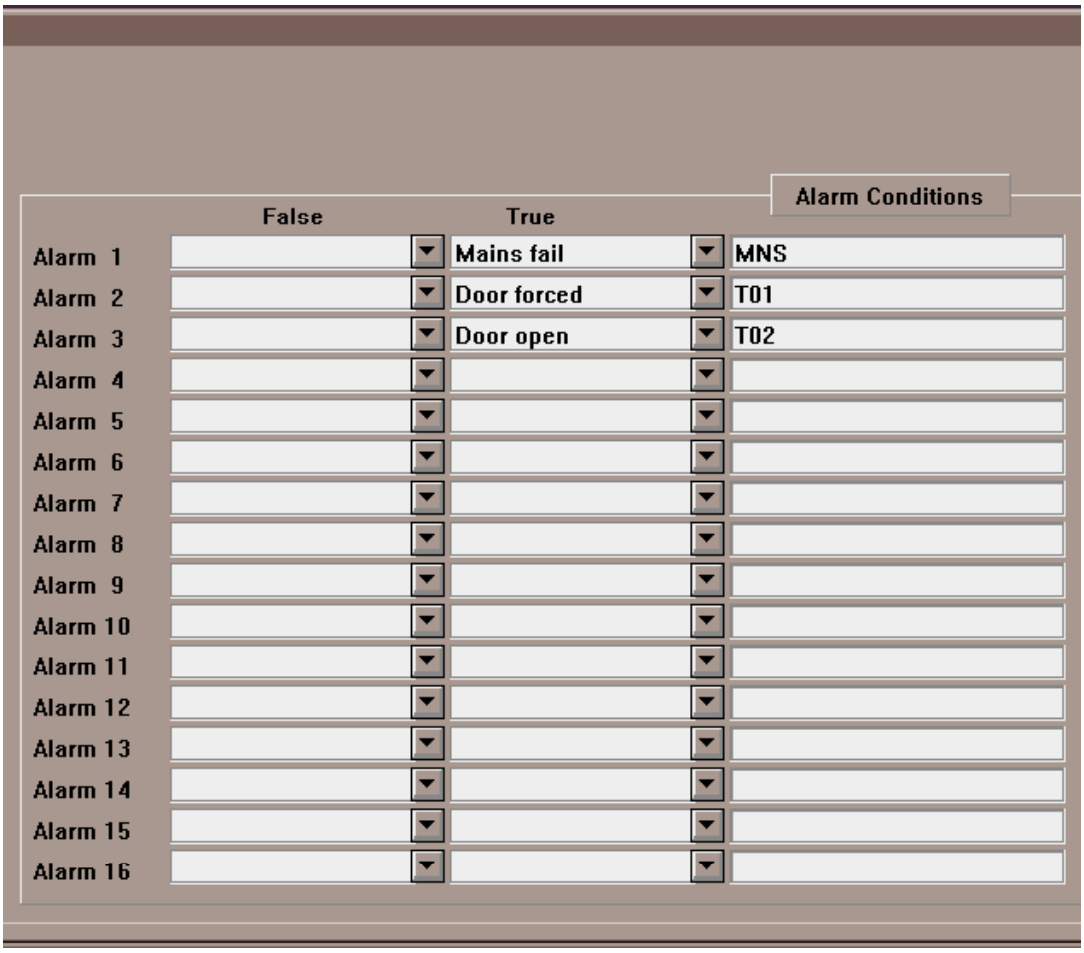


Fig. 18.2 Reader Logic Entry window.

The alarm program line is entered on the light grey line, opposite the relevant Alarm line, the Alarm name is entered into the dark grey bar below. The Alarm name is selected from a drop down menu, thus Alarms and their text messages must be set beforehand, otherwise they will not appear on this menu.

The Timer lines are for internal use only. They control the timing of reader operations. For example, the time allowed to open the door after card removal can be set in this way. The time is selected from a drop down menu, giving a range of 0.0s to 59.9s in 0.1s increments.

The Latch lines allow the setting and resetting of latches.

The Reader System Alarms, cover occurrences such as an invalid card transaction or reader going off-line due to a telemetry failure. These alarms can cause Alarm Windows or Pages to appear on the VISIKEY screen.

The Transaction Verification System allows the checking of a person passing through a turnstile for example, before updating their APB level. The two lines of script used for this facility (Transaction Okay and Transaction Void) only become *TRUE* on the falling edge of a script lines.

Alarm, Output, Input, CCM, Latch and Timer conditions can all be used freely in any expression - but beware - strange results can occur when cross referencing conditions. This can lead to 'oscillations' of outputs and alarms.

Writing a Program

VISIKEY programs are first written using a mnemonic language. This mnemonic language is then entered into the relevant section of the 'Reader Logic' window. The VISIKEY will then tokenise every program line (i.e. a number is assigned to each operator and operand) and these tokens are then sent to the relevant readers. The operands available through the Reader Logic window are:

Description	Label	Token (Hex)	R100 Usage	R500 Usage
Card present	CPR	01	Card present	Card present
Permit access	OPN	02	Permit access	Permit access
Mains fail	MNS	03	Mains fail	Mains fail
Duress button	DUR	04	Duress button	Duress button
Transaction 01	—-	40	Trans Okay	Trans Okay
Transaction 02	—-	41	Trans Void	Trans Void
Set Latch 01	L01	50		
Set Latch 02	L02	51		
Set Latch 03	L03	52		
Set Latch 04	L04	53		
Set Latch 05	L05	54		
Set Latch 06	L06	55		
Set Latch 07	L07	56		
Set Latch 08	L08	57		
Reset Latch 01	L01	60		
Reset Latch 02	L02	61		
Reset Latch 03	L03	62		
Reset Latch 04	L04	63		
Reset Latch 05	L05	64		
Reset Latch 06	L06	65		
Reset Latch 07	L07	66		
Reset Latch 08	L08	67		
Time Zone 01	Z01	70		
Time Zone 02	Z02	71		
Time Zone 03	Z03	72		
Time Zone 04	Z04	73		
Time Zone 05	Z05	74		
Time Zone 06	Z06	75		
Time Zone 07	Z07	76		
Time Zone 08	Z08	77		
Output 01	O01	80	Go Relay	Go Relay
Output 02	O02	81	Tamper	
Output 03	O03	82	Alarm Shunt	

Output 04	O04	83	Unused Entry	
Output 05	O05	84	Door Open	
Output 06	O06	85	Duress	
Output 07	O07	86		
Output 08	O08	87		
Output 09	O09	88		
Output 10	O10	89		
Output 11	O11	8A		
Output 12	O12	8B		
Output 13	O13	8C		
Output 14	O14	8D		
Output 15	O15	8E		
Output 16	O16	8F		
Input 01	I01	90	Door Open	Door Open
Input 02	I02	91	Remote Release	
Input 03	I03	92		
Input 04	I04	93		
Input 05	I05	94		
Input 06	I06	95		
Input 07	I07	96		
Input 08	I08	97		
Input 09	I09	98		
Input 10	I10	99		
Input 11	I11	9A		
Input 12	I12	9B		
Input 13	I13	9C		
Input 14	I14	9D		
Input 15	I15	9E		
Input 16	I16	9F		
Tamper 01	F01	A0	Tamper A	
Tamper 02	F02	A1	Tamper B	
Tamper 03	F03	A2		
Tamper 04	F04	A3		
Tamper 05	F05	A4		
Tamper 06	F06	A5		
Tamper 07	F07	A6		
Tamper 08	F08	A7		
Tamper 09	F09	A8		
Tamper 10	F10	A9		
Tamper 11	F11	AA		
Tamper 12	F12	AB		
Tamper 13	F13	AC		
Tamper 14	F14	AD		
Tamper 15	F15	AE		
Tamper 16	F16	AF		
Timer 01	T01	B0		
Timer 02	T02	B1		
Timer 03	T03	B2		
Timer 04	T04	B3		
Timer 05	T05	B4		
Timer 06	T06	B5		
Timer 07	T07	B6		
Timer 08	T08	B7		
Timer 09	T09	B8		
Timer 10	T10	B9		
Timer 11	T11	B10		
Timer 12	T12	B11		

Timer 13	T13	B12		
Timer 14	T14	B13		
Timer 15	T15	B14		
Timer 16	T16	B15		
Alarm 01	A01	C0		
Alarm 02	A02	C1		
Alarm 03	A03	C2		
Alarm 04	A04	C3		
Alarm 05	A05	C4		
Alarm 06	A06	C5		
Alarm 07	A07	C6		
Alarm 08	A08	C7		
Alarm 09	A09	C8		
Alarm 10	A10	C9		
Alarm 11	A11	C10		
Alarm 12	A12	C11		
Alarm 13	A13	C12		
Alarm 14	A14	C13		
Alarm 15	A15	C14		
Alarm 16	A16	C15		
CCM In 01	C01	D0	CCM 1	
CCM In 02	C02	D1	CCM 2	
CCM In 03	C03	D2	CCM 3	
CCM In 04	C04	D3	CCM 4	
CCM In 05	C05	D4	CCM 5	
CCM In 06	C06	D5	CCM 6	
CCM In 07	C07	D6	CCM 7	
CCM In 08	C08	D7	CCM 8	
CCM In 09	C09	D8	CCM 9	
CCM In 10	C10	D9	CCM 10	
CCM In 11	C11	D10	CCM 11	
CCM In 12	C12	D11	CCM 12	
CCM In 13	C13	D12	CCM 13	
CCM In 14	C14	D13	CCM 14	
CCM In 15	C15	D14	CCM 15	
CCM In 16	C16	D15	CCM 16	

Operators

Description	Label	Token (Hex)
AND	&	F0
OR	+	F1
NOT	~	F2
EOR	^	F3

An example of a program line could be:

Output_1 = Input_3 AND NOT Input_5

Now, because of the use of RPN, this would become:

Output_1 = Input_3 Input_5 NOT AND

In the abbreviated mnemonic language this would be:

O01=I03 I05 ~ &

and this is what you would enter into the system.

Once recognised by the VISIKEY, this form would then be tokenised. Tokenising would give:

80 92 94 F2 F0

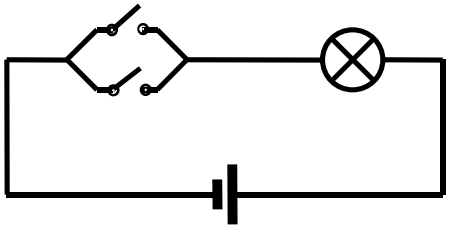
and this is the form in which the program would be sent to the relevant readers.

Appendix 1

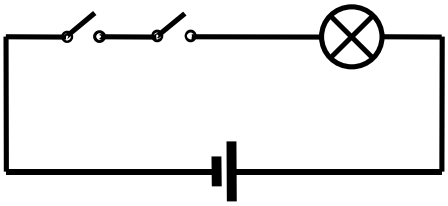
Boolean Algebra (RPN)

This is a system of logical operators based on a binary system. Consider the two electrical circuits shown below:

(i)



(ii)



In (i), the bulb will light if either of the two switches is closed.

In (ii), it will light only if both switches are closed.

We can represent the positions of the switches by a ‘1’ if the switch is closed (i.e. current flows through it) and ‘0’ if the switch is open (no current). Now, for the bulb, we can assign values in the same fashion; a ‘1’ if the bulb is lit (current flows through it) and a ‘0’ if it is not (no current flows).

Using these values, we can tabulate the actions of both circuits:

Circuit (i)		
Switch		Bulb
One	Two	
0	0	0
0	1	1
1	0	1
1	1	1

Circuit (ii)		
Switch		Bulb
One	Two	
0	0	0
0	1	0
1	0	0
1	1	1

We can see that the bulb in circuit (i) will light if either switch 1 OR switch 2 is closed. For circuit (ii), the bulb will light only if switch one AND switch 2 are closed.

Circuit one illustrates the action of what is known in Boolean Algebra as an OR operator.

Circuit 2 acts like an AND operator.

The tables we have made that show their responses are known as truth tables. All possible inputs are entered and the results calculated. The action of a operator is completely described by its truth table.

An OR-operator gives a true result if any of its inputs are true.

An AND-operator gives a true result if, and only if, both inputs are true.

The VISIKEY also allows the use of two more operators, the NOT operator and the Exclusive-OR (EOR) operator.

The NOT operator has only one input and its output is the opposite of this. It inverts the input.

The EOR operator gives a true output (a ‘1’) only if one of the inputs is true. If both, or neither are true then the output is false.

Truth tables for EOR & NOT operators.

EOR		
Input 1	Input 2	Output
0	0	0
0	1	1
1	0	1
1	1	0

NOT	
Input 1	Output
0	1
1	0

Reverse Polish Notation (RPN)

Reverse Polish Notation, although it may at first seem complex, is actually based on a very simple system. Expressions in RPN form show exactly how a calculation will be carried out by a computer.

When carrying out calculations the computer utilises an area of memory known as the STACK. This stack may be regarded as a pile of plates, each of which has a number written on it. Plates may only be removed or placed onto the pile at the very top. Only the number on the topmost plate can be read.

When doing calculations the computer examines the operation to be carried out and then takes a number from the top of the stack. It will then either operate on this number alone e.g. if it is a NOT operation, or it will take the next number from the stack, which has now risen to the top, and combine it with the previous number e.g. for AND, OR and EOR operations. The result of this operation, on either one, or two numbers (operands) is then placed ('pushed') onto the stack at the top.

Other numbers can then be added to the top of the stack, and the result will sink down (but not be forgotten), or the result can be used immediately in another calculation. You must think in this form when converting expressions into Reverse Polish Notation.

Some examples:

Infix form	RPN form
1+2	1 2 +
2x3	2 3 x
4/5	4 5 /
5/4	5 4 /

A AND B	A B AND
NOT A AND (B OR C)	B C OR A NOT AND
T01 AND NOT A01	T01 A01 NOT AND

The examples given here should be sufficient for the needs of VISIKEY reader programming, but for a fuller explanation of RPN consult a more expansive computing text.

Example script program.

Suppose we wanted to open a door for 5 seconds when either a valid card is presented to

a reader assigned to the door or the request to exit button is pressed.

Assuming:-

The door lock is connected to output 1.

The request to exit button is connected to CCM input 1.

We need a timer to provide the 5 second unlock time, for this we will use timer 1.

The easy way to do this is in 3 steps.

1. Write down the Boolean logic required, this would be:-

Output 1 = Timer 1	; This unlocks the door for the duration ; of Timer 1
Timer 1 = CCM Input 1 OR Valid Card Presented	; This sets Timer 1 true if Input 1 is true ; or if a Valid Card is Presented at the reader

2. Convert the Boolean logic from step 1 into script lables. These lables are taken from the above list.

Therefore:

Boolean Logic	Script Lables
Output 1 = Timer 1	O01 = T01
Timer 1 = CCM Input 1 OR Valid Card Presented	T01 = C01 + OPN

3. We now have the logic required for the script

i.e. O01 = T01
T01 = C01+OPN

These need to be converted to RPN Logic before they can be entered into VisiKey.

Therefore:

Boolean Logic	RPN Logic
O01=T01	O01=T01
T01=C01+OPN	T01=C01OPN+

It is now simply a matter of entering the above RPN logic into VisiKey.

Select the reader logic library, this is in the config menu (reader logic). Referring to figure 1, enter a name for the reader logic in the next free logic space (we have used the name example as logic 3) and then press the selection box to the right of the name entered.

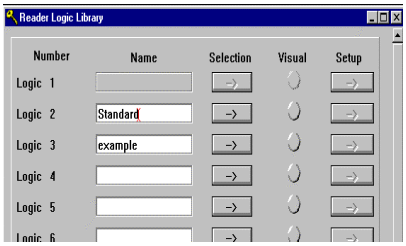


Figure 1.

Referring to figure 2, we are now in the logic editor, here we simply enter the RPN logic we developed in step 3.

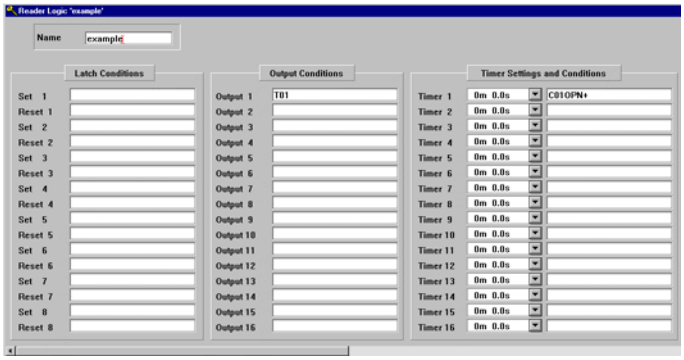
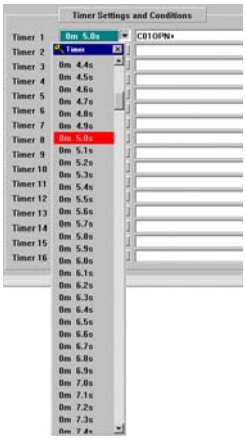


Figure 2.

The final Step is to set the duration for Timer 1, this is done by selecting the drop down list of available timer durations (by clicking on the grey box beside the white box which shows 0m 0.0s) and scrolling down the list selecting 0m 5.0s. Refer to figure 3.


Timer Settings and Conditions
Timer 1
Timer 2
Timer 3
Timer 4
Timer 5
Timer 6
Timer 7
Timer 8
Timer 9
Timer 10
Timer 11
Timer 12
Timer 13
Timer 14
Timer 15
Timer 16
0m 5.0s
C010PN=
Timer
0m 4.4s
0m 4.5s
0m 4.6s
0m 4.7s
0m 4.8s
0m 4.9s
0m 5.0s
0m 5.1s
0m 5.2s
0m 5.3s
0m 5.4s
0m 5.5s
0m 5.6s
0m 5.7s
0m 5.8s
0m 5.9s
0m 6.0s
0m 6.1s
0m 6.2s
0m 6.3s
0m 6.4s
0m 6.5s
0m 6.6s
0m 6.7s
0m 6.8s
0m 6.9s
0m 7.0s
0m 7.1s
0m 7.2s
0m 7.3s
Figure 3.

Appendix 2

Plan and Map Script Language

The VISIKEY can display real time depiction's of buildings and sites. To create a plan or map, a standard text editor is required to enter the PDL (Page Description Language). Here follows a list of commands available:

; (comment)

The permits an entry of a comment with the description.

Circle (fill) (line) <area> <x-pos1> <y-pos1> <x-pos2> <y-pos2>

Draws a lined and/or filled circle.

Colour <fore-col> <back-col>

Sets the foreground and background colours.

Line <area> <x-pos1> <y-pos1> <x-pos2> <y-pos2>

Draws a line between to points.

Origin <x-pos> <y-pos>

Sets the origin - defaults to (0,0).

Reader <loop> <reader> <x-pos1> <y-pos1> <x-pos2> <y-pos2>

Draws a reader.

Rectangle (fill) (line) <area> <x-pos1> <y-pos1> <x-pos2> <y-pos2>

Draws a lined and/or filled rectangle.

Text <area> <x-pos> <y-pos> <point-size> <text>

Draws text of a defined size.

The entries in each command are described as follows:

Area

An Area number from 0 to 127 (for Areas 1 to 128).

Loop

A Loop number from 0 to 17 (for Loops 1 to 18).

Reader

A Reader number from 0 to 127 (for Readers 1 to 128).

Fore-Col & Back-Col

A colour number from 0 to 15.

Point-Size

A point size from 1 to 63.

X- and Y- Co-ordinates

A co-ordinate value from 0 to 4095.

Fill and Line

Whether a shape has a filled interior and/or an outline.

Appendix 3

Glossary of terms

VISIKEY - Access Control System, i.e. the VISIKEY.

Access Rights - The Area and time limits of access assigned to a Department.

Alarm - An alert indicating abnormal system condition e.g. a fire-alarm.

Alarm window - window that allows the custom setting of alarm messages (including instructions) e.g. 'Fire!! - alert emergency services.'

AND - a logical operator in Boolean Algebra which only gives a true result if both inputs are true.

Anti-Passback - a security feature which prevents card/tag sharing and lending by employees. Abbreviated to APB.

Anti-Passback level - the operator defined security level of an Area. A higher number means a higher level. All lower levels must have been entered before access to the next level is allowed.

APB - Anti-Passback Area - a pre-defined set of physical limits within a building e.g. store-room, laboratory. Defined by the readers on its outer periphery.

Back-up - a second copy of a file, or set of files kept for added security. Usually kept on a physical medium i.e. a hard-disc or on paper.

Backing-up time - the interval at which the VISIKEY automatically makes back-up copies of its files.

Bit-switches - small switches which can be set manually within devices to control device response.

BMS - Building Management System.

Boolean Algebra - a system of combining inputs to give outputs using logical operations.

Card-reader - a device for reading the key-number of cards and relaying this information to the VISIKEY computer. The reader can then allow or deny access according to central instruction.

Capacity - the number of persons currently in an Area.

Capacity limit - the maximum number of persons allowed in that Area.

Clicking - selecting an icon by pressing and releasing a mouse button.

Close icon - clicking on this closes a window.

Cursor - indicates the position where the next typed character will appear on the screen. It is depicted as a red line in the VISIKEY.

Day Type - the name of a day which has been previously defined in terms of up to eight time-zones.

Department - an employee group with the same, pre-set, Access Rights e.g. Management, Engineering.

Dragging - moving a window about the screen by clicking and holding on the Title bar. The pointer icon changes to a hand. Dragging allows the custom positioning of windows on the monitor.

Duress PIN - Pressing the ‘E’ key while a card is still in a reader sets off the Duress alarm, informing the operator that the user is acting under threat.

EOR - a logical operator used in Boolean Algebra. Gives a true output if one, and only one, of its inputs is true.

EPROM - Erasable Programmable Read Only Memory.

Holiday information - operator configurable information which can override pre-set Access Rights on specific dates.

Icon - a small displayed graphic which performs a specific operation when selected e.g. the CLOSE icon.

Keycard - a plastic card with an attached magnetic strip. This strip holds the users key-number, which is read by the card reader when the Keycard is inserted.

I/0 - Input/Output. The operations by which the system receives information from and sends information to other devices.

Key-holder - a person who holds either a Keycard or an IR-tag.

Key-number - the 16-digit identifying number of a user.

LED - Light Emitting Diode. A small light emitting device.

Login (or Log-in) - the action whereby an operator enters their user name and Password to inform the VISIKEY that they wish to use the system as a system operator.

Logout (or Log-out) - the action performed when leaving the VISIKEY to inform it that an operator has left the system.

Loop - a series of readers physically linked by a common communication system.

LSB - Least Significant Bit.

Megabyte - (Mbyte or Mb) one million bytes of possible information storage space. Effectively, storage space for one million characters.

Menu - a display of a number of selectable options.

Mouse - a pointing device which controls the pointer when moved across a smooth surface. Has one or more buttons to allow ‘clicking’ and ‘Dragging’.

MROC - Manual Reader Override Command. Allows direct control of a reader, or set of readers, by a VISIKEY operator.

MSB - Most Significant Bit.

Multiplexor - a device which allows and controls the connection of many communications lines.

Multi-User - allows several console operators to concurrently access the VISIKEY.

MUX - An abbreviation for Multiplexor.

NOT-gate - a Boolean operator which gives the inverse of its input as the output.

Off-line reader - a card or tag-reader which has control over its own function i.e. it can decide Access Rights without needing to consult the central VISIKEY database.

On-line reader - a card or tag-reader which consults the VISIKEY central database before allowing or denying entry.

Operator - a person with the right to control the VISIKEY. The level of control allowed can be set through the SYSTEM menu.

OR-gate - a Boolean operator which gives a true output if either, or both, of its inputs are true.

Packing - the process of increasing VISIKEY efficiency by compacting the key-holder database and removing any records no longer required.

Password - the secret word, unique to each operator, which ensures that the VISIKEY is aware of who is operating the system at any given time. It is entered when Logging on.

PC - Personal Computer. Usually implies an IBM or compatible machine.

PIN - Personal Identification Number. This number is typed into a keypad on readers as necessary. It is unique to each user and each user should keep their PIN secret.

PIN algorithm - a method of automatically assigning PINs to users.

Pointer - the on-screen arrow icon which is controlled by the pointing device.

PRINT icon - opens a print options window, allowing the printing of a window contents.

Quit - an option which allows the computer to leave the VISIKEY completely. It is not recommended that you do this as system security may be compromised.

RAM - Random Access Memory. Memory in which changeable information can be stored.

Reader - a card-reader or tag-reader.

Reader Logic - the series of programmed lines which controls the physical operation of a particular reader or group of readers.

Reader Resources - a lookup table allocation physical I/O on a DPU to logical I/O within individual logical readers.

RPN - Reverse Polish Notation. See ‘Programming a Reader’ and Appendix 4.

Single-User - allows only one console operator to access the VISIKEY.

Supervisor - the default user name of a VISIKEY operator with complete access to all system functions.

Tag-reader - a reader which reads the Keynumber from IR-tags.

Technology - the reader input medium e.g. Keycards or IR-tags.

Title-bar - the bar at the top of a window which displays the window name. it is also a drag icon, allowing the window to be positioned as desired by the operator.

Tokenise - to convert a program or other expression (e.g. a Boolean expression) into a form containing only numbers.

Trackerball - a device which controls the on-screen pointer using a ball which is moved by the operator.

User - a Keycard Holder.

VGA - the video display standard which is used on the VISIKEY.

Watermark card - see Appendix 3.

Week Type - the name of a week which has had each day in it defined in terms of Day Types.

Window - an area on the screen which allows access to, and manipulation of, stored information.

Window sizing icon - an icon which allows the window to be re-sized to the most convenient dimensions.

Year Type - the name of a year which has had each week in it defined in terms of Week Types.